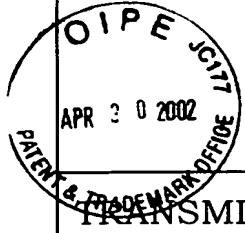
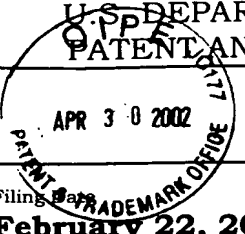
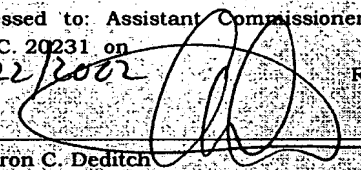


#4

			
TRANSMITTAL		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	
Application Number 10/080,647		Docket Number: 10746/31	Examiner Not Yet Assigned
Filing Date February 22, 2002		Art Unit 2131	Inventor(s) HORITA et al.
Invention Title DISTRIBUTED DIGITAL SIGNATURE GENERATION METHOD AND DIGITALLY SIGNED DIGITAL DOCUMENT GENERATION METHOD AND APPARATUS			

Assistant Commissioner
for Patents
Washington, DC 20231

I hereby certify that this correspondence is being deposited with
the United States Postal Service as first class mail in an
envelope addressed to: Assistant Commissioner for Patents,
Washington, D.C. 20231 on
Date: 4/22/2002 Reg. No. 33,865
Signature: 
Aaron C. Deditch

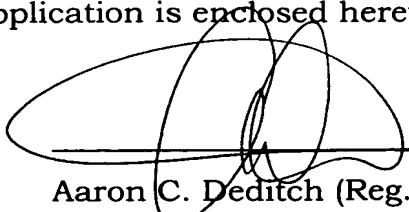
CLAIM TO CONVENTION PRIORITY UNDER 35 U.S.C. 119

S I R :

Claim to Convention Priority Date of Japanese Patent
Application No. 2001-047338, filed in Japan on February 22, 2001, was
made at the time this United States application was filed. In order to
complete the claim to Convention Priority Date under 35 U.S.C. 119, a
certified copy of this Japanese Application is enclosed herewith.

Dated:

4/22/2002


Aaron C. Deditch (Reg. No. 33,865)

KENYON & KENYON
One Broadway
New York, N.Y. 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)
CUSTOMER NO. 26646

© Kenyon & Kenyon 2002



PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy
of the following application as filed with this office.

Date of Application: February 22, 2001

Application Number: No. 2001-047338
[ST.10/C]: [JP 2001-047338]

Applicant(s) NIPPON TELEGRAPH AND TELEPHONE
CORPORATION

March 15, 2002

Commissioner,
Patent Office

Kouzo Oikawa (Seal)

Certificate No.2002-3016959



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 2月22日

出 願 番 号

Application Number:

特願2001-047338

[ST.10/C]:

[JP2001-047338]

出 願 人

Applicant(s):

日本電信電話株式会社

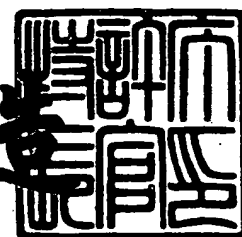
CERTIFIED COPY OF
PRIORITY DOCUMENT

Best Available Copy

2002年 3月15日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 NTTH126715

【提出日】 平成13年 2月22日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 G09C 1/00

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 堀田 英一

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 小野 諭

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100070150

【弁理士】

【氏名又は名称】 伊東 忠彦

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項 1】 デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名作成方法において、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、

入力されるデジタル文書のハッシュ値に対して前記部分署名鍵を用いて、各々の部分デジタル署名を作成し、

各々のデジタル署名装置において、作成された前記部分デジタル署名或いは入力された前記デジタル文書と該部分デジタル署名の組を出力し、

各デジタル署名装置から出力された前記部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成することを特徴とする分散デジタル署名作成方法。

【請求項 2】 入力された前記デジタル文書に対して複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、前記統合デジタル署名を作成するために施す各部分デジタル署名の前記変換処理の処理量を最小化する請求項 1 記載の分散デジタル署名作成方法。

【請求項 3】 前記部分デジタル署名を前記閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分デジタル署名の存在を判定し、かつ不正な部分デジタル署名を特定する請求項 1 記載の分散デジタル署名作成方法。

【請求項 4】 デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名作成方法において、

各々の署名装置に対して、入力されるデジタル文書に、各々 1 個以上の付加情報を付加して 1 個以上の付加情報付デジタル文書を出力し、

信頼される第三者機関を用いることなく、各々の署名装置において部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、

前記付加情報付デジタル文書のハッシュ値に対して前記部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、

前記付加情報付デジタル文書と前記部分デジタル署名の組を出力し、

各デジタル署名装置から出力された前記付加情報付デジタル文書と、部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成することを特徴とする分散デジタル署名作成方法。

【請求項5】 入力された前記デジタル文書に対して複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、前記統合デジタル署名を作成するために施す各部分デジタル署名の前記変換処理の処理量を最小化する請求項4記載の分散デジタル署名作成方法。

【請求項6】 前記部分デジタル署名を前記閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分デジタル署名の存在を判定し、かつ不正な部分デジタル署名を特定する請求項4記載の分散デジタル署名作成方法。

【請求項7】 デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置であって、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるデジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分デジタル署名を作成し、作成された該部分デジタル署名或いは入力された該デジタル文書と該部分デジタル署名の組を出力する複数の部分デジタル署名作成手段と、

出力された前記部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成手段とを有す

ることを特徴とする分散デジタル署名作成装置。

【請求項 8】 前記統合デジタル署名作成手段は、

入力された前記デジタル文書に対して複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、前記統合デジタル署名を作成するために施す各部分デジタル署名の前記変換処理の処理量を最小化する手段を含む請求項 7 記載の分散デジタル署名作成装置。

【請求項 9】 前記統合デジタル署名作成手段は、

前記部分デジタル署名を前記閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分デジタル署名の存在を判定し、かつ不正な部分デジタル署名を特定する手段を含む請求項 7 記載の分散デジタル署名作成装置。

【請求項 10】 デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置であって、

各々の署名装置に対して、入力されるデジタル文書に、各々 1 個以上の付加情報を付加して 1 個以上の付加情報付デジタル文書を出力する付加情報結合手段と、

信頼される第三者機関を用いることなく、各々の署名装置において部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、前記付加情報付デジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、該付加情報付デジタル文書と前記部分デジタル署名の組を出力する複数の部分デジタル署名作成手段と、

出力された前記付加情報付デジタル文書と、前記部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成手段とを有することを特徴とする分散デジタル署名作成装置。

【請求項 11】 前記統合デジタル署名作成手段は、

入力された前記デジタル文書に対して複数ある部分署名機関が作成した部分

デジタル署名を閾値個数集めることにより、前記統合デジタル署名を作成するために施す各部分デジタル署名の前記変換処理の処理量を最小化する手段を含む請求項10記載の分散デジタル署名作成装置。

【請求項12】 前記統合デジタル署名作成手段は、

前記部分デジタル署名を前記閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分デジタル署名の存在を判定し、かつ不正な部分デジタル署名を特定する手段を含む請求項10記載の分散デジタル署名作成装置。

【請求項13】 デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名付デジタル文書作成方法において、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、

入力されるデジタル文書のハッシュ値に対して前記部分署名鍵を用いて、各々の部分デジタル署名を作成し、

各々のデジタル署名装置において、作成された前記部分デジタル署名或いは入力された前記デジタル文書と該部分デジタル署名の組を出力し、

各デジタル署名装置から出力された前記部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成し、

入力されたデジタル文書と、作成された前記統合デジタル署名とを含むデジタル署名付デジタル文書を作成することを特徴とするデジタル署名付デジタル文書作成方法。

【請求項14】 デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名付デジタル文書作成方法において、

各々の署名装置に対して、入力されるデジタル文書に、各々1個以上の付加情報を付加して1個以上の付加情報付デジタル文書を出力し、

信頼される第三者機関を用いることなく、各々の署名装置において部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、

前記付加情報付デジタル文書のハッシュ値に対して前記部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、

前記付加情報付デジタル文書と前記部分デジタル署名の組を出力し、

各デジタル署名装置から出力された前記付加情報付デジタル文書と、部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成し、

生成された前記付加情報付デジタル文書と作成された前記統合デジタル署名とを含むデジタル署名付デジタル文書を作成することを特徴とするデジタル署名付デジタル文書作成方法。

【請求項 15】 デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名付デジタル文書作成装置であって、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるデジタル文書のハッシュ値に対して前記部分署名鍵を用いて、各々の部分デジタル署名を作成し、作成された前記部分デジタル署名或いは入力された前記デジタル文書と該部分デジタル署名の組を出力する複数の部分デジタル署名作成手段と、

各デジタル署名装置から出力された前記部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成手段と、

入力されたデジタル文書と、作成された前記統合デジタル署名とを含むデジタル署名付デジタル文書を作成する文書作成手段とを有することを特徴とするデジタル署名付デジタル文書作成装置。

【請求項 16】 デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名付デジタル文書作成装置であって、

各々の署名装置に対して、入力されるデジタル文書に、各々 1 個以上の付加情報を付加して 1 個以上の付加情報付デジタル文書を出力する付加情報結合手

段と、

信頼される第三者機関を用いることなく、各々の署名装置において部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、前記付加情報付デジタル文書のハッシュ値に対して前記部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、該付加情報付デジタル文書と前記部分デジタル署名の組を出力する部分デジタル署名作成手段と、

各デジタル署名装置から出力された前記付加情報付デジタル文書と、部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成手段と、

生成された前記付加情報付デジタル文書と作成された前記統合デジタル署名とを含むデジタル署名付デジタル文書を作成する文書作成手段とを有することを特徴とするデジタル署名付デジタル文書作成装置。

【請求項 17】 デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置に実行させる分散デジタル署名作成プログラムであって、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるデジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分デジタル署名を作成し、作成された該部分デジタル署名或いは入力された該デジタル文書と該部分デジタル署名の組を出力する部分デジタル署名作成プロセスと、

出力された前記部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成プロセスとを有することを特徴とする分散デジタル署名作成プログラム。

【請求項 18】 デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置に実行させる分散デジタル署名作成プロ

グラムであって、

入力されるデジタル文書に、各々1個以上の付加情報を付加して1個以上の付加情報付デジタル文書を出力する付加情報結合プロセスと、

信頼される第三者機関を用いることなく、部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、前記付加情報付デジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、該付加情報付デジタル文書と前記部分デジタル署名の組を出力する複数の部分デジタル署名作成プロセスと、

出力された前記付加情報付デジタル文書と、前記部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成プロセスとを有することを特徴とする分散デジタル署名作成プログラム。

【請求項19】 デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置に実行させる分散デジタル署名作成プログラムを格納した記憶媒体であって、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるデジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分デジタル署名を作成し、作成された該部分デジタル署名或いは入力された該デジタル文書と該部分デジタル署名の組を出力する部分デジタル署名作成プロセスと、

出力された前記部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成プロセスとを有することを特徴とする分散デジタル署名作成プログラムを格納した記憶媒体。

【請求項20】 デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置に実行させる分散デジタル署名作成プロ

グラムを格納した記憶媒体であって、

入力されるデジタル文書に、各々 1 個以上の付加情報を付加して 1 個以上の付加情報付デジタル文書を出力する付加情報結合プロセスと、

信頼される第三者機関を用いることなく、部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、前記付加情報付デジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、該付加情報付デジタル文書と前記部分デジタル署名の組を出力する複数の部分デジタル署名作成プロセスと、

出力された前記付加情報付デジタル文書と、前記部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成プロセスとを有することを特徴とする分散デジタル署名作成プログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体に係り、特に、デジタル文書に対するデジタル署名を作成するサービスにおいて、あるデジタル文書に対して、そのデジタル署名が存在するとき、当該デジタル署名が偽造されたものではないこと、即ち、当該デジタル署名が他の手段で作成されたものではないことを保証するための署名作成において、公開鍵暗号方式を用いた分散署名を複数の部分デジタル署名機関が独立して行ない、分散署名機関で作成された部分デジタル署名から一つの統合デジタル署名を得るための分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体に関する。

【0002】

詳しくは、複数ある分散署名機関のうち、一定数までのものが部分デジタル署名作成時に不正な処理を行っても、その部分デジタル署名から正しい統合デジタル署名を得るための分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体に関する。

【0003】

また、集中型のデジタル署名における秘密鍵の盗難などの危険性を排除するための分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体に関する。

【0004】

また、一つの統合デジタル署名を得るために複数ある分散部分デジタル署名機関のうち、すべてのものが正しい部分デジタル署名を作成しなければならないような従来型の分散型署名装置の耐攻撃性及び耐故障性における弱点を排除するための分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体に関する。

【0005】

【従来の技術】

従来の公開鍵暗号方式に基づく分散デジタル署名作成システムの多くは、分散された各々の部分デジタル署名作成システムが部分デジタル署名に用いる署名鍵を生成する際に、信頼される第三者機関を用いる。この場合、この第三者機関から署名鍵についての情報が漏洩する可能性があり、システムの中の一か所が秘密を漏洩するとシステムの安全性が全面的に損なわれるという弱点、即ち、秘密漏洩の単一点が存在するという弱点がある。

【0006】

また、複数ある分散署名機関の全てのものが正しい部分デジタル署名を作成しなければ部分デジタル署名からデジタル署名を作成できないような分散デジタル署名作成システムにおいては、複数ある分散署名機関の中で1つでも不

正な動作をするとデジタル署名が作成できないという耐攻撃性及び、耐故障性における弱点を有している。

【0007】

上記のような、秘密漏洩上の弱点および耐郡家紀勢及び耐故障性における弱点を克服する分散デジタル署名作成システムとしては、『T.Wu et al.: 「Building intrusion tolerant applications」, in Proceedings of 8th UNENIX Security Symposium, USENIX, 1999』（以下、第1の従来の方法）に報告されているものがある。当該システムは、部分デジタル署名に用いる署名鍵を第三者機関を用いることなく、分散された複数の部分デジタル署名作成機関の全体が分散処理により、各々の部分デジタル署名作成機関を用いる部分署名鍵を作成し、さらに、それらの部分署名鍵についての部分的な情報を互いに交換することにより、複数ある部分デジタル署名作成機関のうちの閾値と呼ばれる一定数のものが正常に動作すれば分散デジタル署名作成を実行することができるシステムとなっている。

【0008】

また、鍵情報が増大することを防ぐ方法として、『S.Miyazaki, K.Sakurai, M.Yung 「On threshold RSA-signing with no dealer」 in Proceedings of ICIS C'99, pp.197-207, Springer, 1999』により提案されている。

また、信頼される第三者機関を用いるものではあるが、閾値個数の部分デジタル署名を組み合わせる統合デジタル署名を作成する方法で、かつ鍵情報が増大するという問題を解決する方法が、『V.Shoup 「Practical threshold signatures」, in Proceedings of Eurocrypt 2000.』（以下、第3の従来の方法）に提案されている。

【0009】

また、特願平8-351565「階層を有する鍵管理方式及び暗号システム、分散デジタル署名システム」（以下、第4の従来の方法）では、階層構造を持つような秘密鍵の閾値分散を用いた分散デジタル署名システムが提案されている。この方式における秘密鍵の閾値分散の方法は、『R.L. Rivest, A. Shamir, and L. Adleman 「A method for obtaining digital signature and public key

cryptosystems」Communications of ACM, Vol.21, pp.294-299, 1978」によるものであり、デジタル署名を分散処理により作成するために、多項式補完式により元の秘密鍵を一度計算する方法をとっている。

【0010】

また、公開鍵暗号方式に基づく分散処理機関を用いてデジタル文書に時刻印を押すサービスとして、特願平11-247994号「分散型時刻認証装置及び方法と分散時刻認証プログラムを記録した記録媒体」（以下、第5の従来の方法）がある。当該文献で提案されている方式で実現する機能は、入力されたデジタル文書に付加する付加情報として時刻を用いることにより実現することができる。この分散型時刻認証装置は、一つの総合時刻署名を得るために複数ある分散時刻署名機関のうち全てのものが正しい部分時刻署名を作成しなければならないという特徴と、複数ある分散時刻署名機関のうちの一部が不正であれば、正しい時刻証明書が発行できないという特徴を有しており、一部の分散時刻署名機関による時刻証明書の偽造を防止する手段を提供している。

【0011】

【発明が解決しようとする課題】

しかしながら、上記第1の従来の方法では、複数ある部分デジタル署名作成システムのうちの閾値個数のどのグループが署名を作成するかに応じて、各部分デジタル署名作成機関が用いる異なる部分署名鍵を用意する必要があり、そのため鍵情報が増大するという問題がある。

【0012】

当該システムにおけるもう一つの問題点は、閾値個数のあるグループでデジタル署名を作成しようとして、その中の一部が正常に機能しないため署名作成に失敗した場合には、他の閾値個数のグループで署名を実行する必要があり、複数ある部分デジタル署名作成機関における部分デジタル署名の作成の処理量、及び統合デジタル署名作成機関と複数ある部分デジタル署名作成機関の間の通信が増大するということである。

【0013】

また、上記第2の従来の方法は、第1の従来の方法の2つの問題点のうち鍵情

報が増大するという問題点を克服することは可能であるが、しかし、この方法においても部分デジタル署名機関の閾値個数のあるグループが署名作成に失敗した場合に、部分デジタル署名作成の処理量及び統合デジタル署名作成機関と複数ある部分デジタル署名作成機関の間の通信量が増大するという第2の問題点は残されている。また、部分デジタル署名からデジタル署名を作成する処理量が部分デジタル署名作成機関の数が増えるに従って増大し、署名作成処理全体の処理量が大きくなるということも問題である。また、部分デジタル署名の正当性を検証するための処理量が大きく、そのため作成された統合デジタル署名が正しい部分署名鍵から作成された部分デジタル署名のみを組み合わせで作られたものであることを保証するための処理量が大きいことも問題である。

【 0 0 1 4 】

また、上記第3の従来の方法は、閾値個数の部分デジタル署名を組み合わせで統合デジタル署名を作成する方法で、かつ鍵情報が増大するという問題を解決することはできるが、当該方法においても部分デジタル署名からデジタル署名を作成する処理量が部分デジタル署名機関の数が増えるに従って増大し、署名作成処理全体の処理量が大きくなるという問題がある。また、部分デジタル署名が正しい部分署名鍵から作成された部分デジタル署名のみを組み合わせで作られたものであることを保証するための処理量が大きいことも問題である。

また、上記第4の従来の方法は、デジタル署名を分散処理により作成するために、多項式補完式により元の秘密鍵を一度計算する方法をとっているため、この計算を実行する機関は秘密鍵の情報を知ることができ、秘密漏洩の単一点が存在するという弱点を伴うものとなっている。また、この文献においては、複数ある秘密価値の部分情報の保持機関が所定の数集まってデジタル署名の生成を試みる際に、それらの部分情報保持者の一部が不正な処理を行う場合に、どの部分情報保持機関が不正を働いたかを識別し、その不正な機関を除いて正しい機関のみで効率的にデジタル署名を生成する方法については、述べられていない。

【 0 0 1 5 】

また、上記第5の従来の方法における分散型時刻認証装置は、複数のある分散時刻署名機関の中で1つでも不正な動作をすると時刻証明書が作成できないとい

う点が耐攻撃性及び耐故障性における弱点となっている。

【 0 0 1 6 】

本発明は、上記の点に鑑みなされたもので、従来の信頼される第三者機関を用いた分散デジタル署名作成システムが持つ、秘密漏洩の単一点が存在するという問題点を解決し、かつ複数ある部分デジタル署名機関のすべてのものが正しい部分デジタル署名を作成しなければ部分デジタル署名からデジタル署名を作成できないような分散デジタル署名作成システムを持つ、複数ある分散署名機関の中で1つでも不正な動作をするとデジタル署名が作成できないという耐攻撃性及び耐故障性における弱点を解決した分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体を提供することを目的とする。

【 0 0 1 7 】

また、本発明の目的は、入力されたデジタル文書に対して、複数ある部分デジタル署名機関が作成した部分デジタル署名を閾値個数集めることにより、当該デジタル文書に対するデジタル署名を作成する閾値分散署名システムにおける、複数ある部分デジタル署名機関の閾値個数のあるグループが署名の作成に失敗した場合に、部分デジタル署名作成の処理量及び統合デジタル署名作成機関と複数ある部分デジタル署名作成機関の間の通信が増大するという問題点を解決した分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体を提供することである。

【 0 0 1 8 】

更なる本発明の目的は、部分デジタル署名からデジタル署名を作成するための処理量が大いという問題を解決した分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体を提供することである。

【 0 0 1 9 】

また、更なる目的は、作成されたデジタル署名が正しい部分署名鍵から作成された部分デジタル署名のみを組み合わせで作られたという意味で正しいものであることを保証するための処理量が多いという問題点を解決した分散デジタル署名作成方法及び装置及び分散デジタル署名付デジタル文書作成方法及び装置及び分散デジタル署名作成プログラム及び分散デジタル署名作成プログラムを格納した記憶媒体を提供することである。

【 0 0 2 0 】

【課題を解決するための手段】

図 1 は、本発明の原理を説明するための図である。

【 0 0 2 1 】

本発明（請求項 1）は、デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名作成方法において、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し（ステップ 1）、

入力されるデジタル文書のハッシュ値に対して部分署名鍵を用いて、各々の部分デジタル署名を作成し（ステップ 2）、

各々のデジタル署名装置において、作成された部分デジタル署名或いは入力されたデジタル文書と該部分デジタル署名の組を出力し（ステップ 3）、

各デジタル署名装置から出力された部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する（ステップ 4）。

【 0 0 2 2 】

本発明（請求項 2）は、入力されたデジタル文書に対して複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、統合デジタル署名を作成するために施す各部分デジタル署名の変換処理の処理量を最小化する。

【 0 0 2 3 】

本発明（請求項 3）は、部分デジタル署名を閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分デジタル署名の存在を判定し、かつ不正な部分デジタル署名を特定する。

【 0 0 2 4 】

本発明（請求項 4）は、デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名作成方法において、

各々の署名装置に対して、入力されるデジタル文書に、各々 1 個以上の付加情報を付加して 1 個以上の付加情報付デジタル文書を出力し、

信頼される第三者機関を用いることなく、各々の署名装置において部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、

付加情報付デジタル文書のハッシュ値に対して部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、

付加情報付デジタル文書と部分デジタル署名の組を出力し、

各デジタル署名装置から出力された付加情報付デジタル文書と、部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する。

【 0 0 2 5 】

本発明（請求項 5）は、入力されたデジタル文書に対して複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、統合デジタル署名を作成するために施す各部分デジタル署名の変換処理の処理量を最小化する。

【 0 0 2 6 】

本発明（請求項 6）は、部分デジタル署名を閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分デジタル署名の存在を判定し、かつ不正な部分デジタル署名を特定する。

【 0 0 2 7 】

図 2 は、本発明の原理構成図である。

【 0 0 2 8 】

本発明（請求項 7）は、デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置 1 であって、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるデジタル文書 M のハッシュ値に対して該部分署名鍵を用いて、各々の部分デジタル署名 1 6 を作成し、作成された該部分デジタル署名 1 6 或いは入力された該デジタル文書と該部分デジタル署名の組を出力する複数の部分デジタル署名作成手段 1 3 と、

出力された部分デジタル署名 1 6 を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成手段 1 4 とを有する。

【 0 0 2 9 】

本発明（請求項 8）は、統合デジタル署名作成手段 1 4 において、

入力されたデジタル文書に対して複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、統合デジタル署名を作成するために施す各部分デジタル署名の変換処理の処理量を最小化する手段を含む。

【 0 0 3 0 】

本発明（請求項 9）は、統合デジタル署名作成手段 1 4 において、

部分デジタル署名を閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分デジタル署名の存在を判定し、かつ不正な部分デジタル署名を特定する手段を含む。

【 0 0 3 1 】

本発明（請求項 1 0）は、デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置であって、

各々の署名装置に対して、入力されるデジタル文書に、各々 1 個以上の付加情報を付加して 1 個以上の付加情報付デジタル文書を出力する付加情報結合手段と、

信頼される第三者機関を用いることなく、各々の署名装置において部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、付加情報付デジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、該付加情報付デジタル文書と部分デジタル署名の組を出力する複数の部分デジタル署名作成手段と、

出力された付加情報付デジタル文書と、部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成手段とを有する。

【 0 0 3 2 】

本発明（請求項 1 1）は、統合デジタル署名作成手段において、

入力されたデジタル文書に対して複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、統合デジタル署名を作成するために施す各部分デジタル署名の変換処理の処理量を最小化する手段を含む。

【 0 0 3 3 】

本発明（請求項 1 2）は、統合デジタル署名作成手段において、

部分デジタル署名を閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分デジタル署名の存在を判定し、かつ不正な部分デジタル署名を特定する手段を含む。

【 0 0 3 4 】

本発明（請求項 1 3）は、デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名付デジタル文書作成方法において、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、

入力されるデジタル文書のハッシュ値に対して部分署名鍵を用いて、各々の部分デジタル署名を作成し、

各々のデジタル署名装置において、作成された部分デジタル署名或いは入

力されたデジタル文書と該部分デジタル署名の組を出力し、

各デジタル署名装置から出力された部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成し、

入力されたデジタル文書と、作成された統合デジタル署名とを含むデジタル署名付デジタル文書を作成する。

【 0 0 3 5 】

本発明（請求項 1 4）は、デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名付デジタル文書作成方法において、

各々の署名装置に対して、入力されるデジタル文書に、各々 1 個以上の付加情報を付加して 1 個以上の付加情報付デジタル文書を出力し、

信頼される第三者機関を用いることなく、各々の署名装置において部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、

付加情報付デジタル文書のハッシュ値に対して部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、

付加情報付デジタル文書と部分デジタル署名の組を出力し、

各デジタル署名装置から出力された付加情報付デジタル文書と、部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成し、

生成された付加情報付デジタル文書と作成された統合デジタル署名とを含むデジタル署名付デジタル文書を作成する。

【 0 0 3 6 】

本発明（請求項 1 5）は、デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名付デジタル文書作成装置であって、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のた

めに用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるデジタル文書のハッシュ値に対して部分署名鍵を用いて、各々の部分デジタル署名を作成し、作成された部分デジタル署名或いは入力されたデジタル文書と該部分デジタル署名の組を出力する複数の部分デジタル署名作成手段と

各デジタル署名装置から出力された部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成手段と、

入力されたデジタル文書と、作成された統合デジタル署名とを含むデジタル署名付デジタル文書を作成する文書作成手段とを有する。

【0037】

本発明（請求項16）は、デジタル文書に対するデジタル署名を複数の署名装置で分散して作成する分散デジタル署名付デジタル文書作成装置であって、

各々の署名装置に対して、入力されるデジタル文書に、各々1個以上の付加情報を付加して1個以上の付加情報付デジタル文書を出力する付加情報結合手段と、

信頼される第三者機関を用いることなく、各々の署名装置において部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、付加情報付デジタル文書のハッシュ値に対して部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、該付加情報付デジタル文書と部分デジタル署名の組を出力する部分デジタル署名作成手段と

各デジタル署名装置から出力された付加情報付デジタル文書と、部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成手段と、

生成された付加情報付デジタル文書と作成された統合デジタル署名とを含

むデジタル署名付デジタル文書を作成する文書作成手段とを有する。

【 0 0 3 8 】

本発明（請求項 1 7）は、デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置に実行させる分散デジタル署名作成プログラムであって、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるデジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分デジタル署名を作成し、作成された該部分デジタル署名或いは入力された該デジタル文書と該部分デジタル署名の組を出力する部分デジタル署名作成プロセスと、

出力された部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成プロセスとを有する。

【 0 0 3 9 】

本発明（請求項 1 8）は、デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置に実行させる分散デジタル署名作成プログラムであって、

入力されるデジタル文書に、各々 1 個以上の付加情報を付加して 1 個以上の付加情報付デジタル文書を出力する付加情報結合プロセスと、

信頼される第三者機関を用いることなく、部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、付加情報付デジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、該付加情報付デジタル文書と部分デジタル署名の組を出力する複数の部分デジタル署名作成プロセスと、

出力された付加情報付デジタル文書と、部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合ディ

タル署名作成プロセスとを有する。

【 0 0 4 0 】

本発明（請求項 1 9）は、デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置に実行させる分散デジタル署名作成プログラムを格納した記憶媒体であって、

信頼される第三者機関を用いることなく、各々が部分デジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるデジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分デジタル署名を作成し、作成された該部分デジタル署名或いは入力された該デジタル文書と該部分デジタル署名の組を出力する部分デジタル署名作成プロセスと、

出力された部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成プロセスとを有する。

本発明（請求項 2 0）は、デジタル文書に対するデジタル署名を分散処理により作成する分散デジタル署名作成装置に実行させる分散デジタル署名作成プログラムを格納した記憶媒体であって、

入力されるデジタル文書に、各々 1 個以上の付加情報を付加して 1 個以上の付加情報付デジタル文書を出力する付加情報結合プロセスと、

信頼される第三者機関を用いることなく、部分デジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、付加情報付デジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分デジタル署名を作成し、該付加情報付デジタル文書と部分デジタル署名の組を出力する複数の部分デジタル署名作成プロセスと、 出力された付加情報付デジタル文書と、部分デジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分デジタル署名に施し、該変換処理の結果から統合デジタル署名を作成する統合デジタル署名作成プロセスとを有する。

【0041】

上記のように、本発明（請求項1、7、17、19）によれば、入力されるデジタル文書に対して、部分デジタル署名の閾値個数のある集合を用いて統合デジタル署名が作れない場合にも、新たに部分デジタル署名の作成を部分デジタル署名作成手段に依頼することなく、最初に集まった部分デジタル署名の全集合の中から他の閾値個数の集合を選び、統合デジタル署名の作成を行う。これにより、閾値個数のある部分デジタル署名作成手段の集合でデジタル署名を作成しようとして、その中の一部が正常に機能しないため署名の作成に失敗した場合に、複数ある部分デジタル署名作成手段における部分デジタル署名の作成の処理量、及び統合デジタル署名作成機関と複数ある部分署名作成機関の間の通信が増大するという問題点を解決することが可能となる。

【0042】

また、本発明（請求項4、10、18、20）によれば、入力されるデジタル文に付加情報を加えたものに対して部分デジタル署名の閾値個数のある集合を用いて統合デジタル署名が作れない場合にも、新たに部分デジタル署名の作成を部分デジタル署名作成手段に依頼することなく、最初に集まった部分デジタル署名の全集合の中から他の閾値個数の集合を選び、統合デジタル署名の作成を行う。これにより、閾値個数のある部分デジタル署名作成手段の集合でデジタル署名を作成しようとして、その中の一部が正常に機能しないため署名の作成に失敗した場合に、複数ある部分署名作成システムにおける部分デジタル署名の作成の処理量及び、統合デジタル署名作成機関と複数ある部分署名作成機関の間の通信が増大するという問題を解決することが可能となる。

【0043】

また、本発明（請求項2、5、8、11）では、入力されたデジタル文書に対して、複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、当該デジタル文書に対するデジタル署名を作成する閾値分散署名システムにおける、部分デジタル署名からデジタル署名を作成するための処理量が大きいう問題点を解決することが可能となる。

【0044】

また、本発明（請求項 3、9）では、入力されたデジタル文書に対して、複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、該デジタル文書に対するデジタル署名を作成する閾値分散署名システムにおける、作成されたデジタル署名が正しい部分署名鍵から作成された部分デジタル署名のみを組み合わせで作られたという意味で正しいものであることを保証するための処理量が大きいという問題点を解決することが可能となる。

【 0 0 4 5 】

また、本発明（請求項 6、12）は、入力されたデジタル文書に対して、複数ある部分署名機関が作成した部分デジタル署名を閾値個数集めることにより、当該デジタル文書に対するデジタル署名を作成する閾値分散署名システムにおける作成されたデジタル署名が正しい部分署名鍵から作成された部分デジタル署名のみを組み合わせで作られたという意味で正しいものであることを保証するための処理量が大きいという問題点を解決することが可能となる。

【 0 0 4 6 】

また、本発明（請求項 13、15）は、入力されるデジタル文書に対して、デジタル署名付デジタル文書を作成する処理の中で、部分デジタル署名の閾値個数のある集合を用いて統合デジタル署名が作れない場合にも、新たに部分デジタル署名の作成を部分デジタル署名作成手段に依頼することなく、最初に集まった部分デジタル署名の全集合の中から他の閾値個数の集合を選び、統合デジタル署名の作成を行ない、それと入力されたデジタル文書を組み合わせ、デジタル署名付デジタル文書を作成する。これにより、閾値個数のある部分デジタル署名作成手段の集合でデジタル署名を作成しようとして、その中の一部が正常に機能しないため署名の作成に失敗した場合に、複数ある部分署名作成システムにおける部分デジタル署名の作成の処理量、及び統合デジタル署名作成機関と複数ある部分署名作成機関の通信が増大するという問題を解決することが可能となる。

【 0 0 4 7 】

また、本発明（請求項 14、16）は、入力されるデジタル文書に対して、付加情報付デジタル文書を作成し、当該付加情報付デジタル文書に対するデ

ィジタル署名付ィジタル文書を作成する処理の中で、部分ィジタル署名の閾値個数のある集合を用いて、統合ィジタル署名が作れない場合にも、新たに部分ィジタル署名の作成を部分ィジタル署名作成手段に依頼することなく、最初に集まった部分ィジタル署名の全集合の中から他の閾値個数の集合を選び、統合ィジタル署名の作成を行ない、それと入力されたィジタル文書を組み合わせ、ィジタル署名付ィジタル文書を作成する。これにより、閾値個数のある部分ィジタル署名作成手段の集合でィジタル署名を作成しようとして、その中に一部が正常に機能しないための署名の作成に失敗した場合に、複数ある部分署名作成システムにおける部分ィジタル署名の作成の処理量、及び統合ィジタル署名作成機関と複数ある部分署名作成機関の間の通信が増大するという問題を解決することが可能となる。

【0048】

【発明の実施の形態】

本発明は、以下の図3から図5に示す3つの閾値分散ィジタル署名作成装置を提案している。

【0049】

図3は、本発明の閾値分散ィジタル署名作成装置の構成図（その1）である。

【0050】

同図において、分散ィジタル署名作成装置1は、複数の部分ィジタル署名作成部13と、統合ィジタル署名作成部14とを有する。

【0051】

部分ィジタル署名作成部13は、入力されたィジタル文書Mに対して各々独立に部分ィジタル署名

$$S_1(M), \dots, S_r(M)$$

を作成する。

【0052】

統合ィジタル署名作成部14は、数の部分ィジタル署名作成部13₁、…、13_rと、当該複数の部分ィジタル署名作成部13で独立に作成されたm

個の部分デジタル署名

$$S_{r(1)}(M), \dots, S_{r(m)}(M),$$

($k \leq m \leq r$ かつ $1 \leq r(1), \dots, r(m) \leq r$) 及び当該デジタル文書Mを受け取り、予め定めた閾値の個数k個の部分デジタル署名作成部13の識別番号からなる1以上であるs個の集合

$$I_1, \dots, I_s$$

に対して、出力された部分デジタル署名から複数の統合デジタル署名

$$S(M, I_1), \dots, S(M, I_s)$$

を作成する。

【0053】

図4は、本発明の閾値分散デジタル署名作成装置の構成図（その2）である。

【0054】

同図に示すデジタル署名作成装置1は、図3の構成と同様であるが、部分デジタル署名作成部13は、入力されたデジタル文書Mに対して各々独立にデジタル文書と部分デジタル署名の組

$$(M, S_1(M)), \dots, (M, S_r(M))$$

を作成する。

【0055】

また、同図における統合デジタル署名作成部14は、当該デジタル文書Mと、当該複数の部分デジタル署名作成部13で独立に作成された部分デジタル署名のm個の組

$$(M, S_{r(1)}(M)), \dots, (M, S_{r(m)}(M))$$

($k \leq m \leq r$ かつ $1 \leq r(1), \dots, r(m) \leq r$) を受け取り、予め定められている閾値の個数k個の部分デジタル署名作成部13の識別番号からなる1以上であるs個の集合

$$I_1, \dots, I_s$$

に対して、出力された部分デジタル署名から複数の統合デジタル署名

$$S(M, I_1), \dots, S(M, I_s)$$

を作成する。

【0056】

図5は、本発明の閾値分散デジタル署名作成装置の構成図（その3）である。同図において、分散デジタル署名作成装置1は、複数の付加情報結合部12、複数の部分デジタル署名作成部13、及び統合デジタル署名作成部14から構成される。

【0057】

付加情報結合部12は、入力されたデジタル文書Mに対して各々独立に1以上 $v(i)$ 個の付加情報

$$\alpha(i, 1), \dots, \alpha(i, v(i))$$

を作成して、文書Mと、

$$\alpha(i, 1), \dots, \alpha(i, v(i))$$

を結合してできる付加情報付デジタル文書

$$M \parallel \alpha(i, 1), \dots, M \parallel \alpha(i, v(i))$$

を作成する。

【0058】

複数のデジタル署名作成部13 i ($1 \leq i \leq r$) は、付加情報結合部12 1 , ..., 12 r に対して、各々に対応して存在し、付加情報結合部12によって生成された付加情報付デジタル文書

$$M \parallel \alpha(i, 1), \dots, M \parallel \alpha(i, v(i))$$

に対して、各々独立に付加情報付デジタル文書とその部分デジタル署名の組、

$$(M \parallel \alpha(i, 1), S_i(M \parallel \alpha(i, 1))), \dots,$$

$$(M \parallel \alpha(i, v(i)), S_i(M \parallel \alpha(i, v(i))))$$

を作成する。

【0059】

統合デジタル署名作成部14は、当該複数の部分デジタル署名作成部13で独立に作成された付加情報付デジタル文書

$$M \parallel \alpha(i, h(i))$$

とその部分デジタル署名の m 個の組

$(M', Sr(1)(M')) , \dots , (M', Sr(m), (M'))$

で $k \leq m \leq r$ かつ $1 \leq r(1) , \dots , r(m) \leq r$ かつ

$M' \in \{M \parallel \alpha(r(i), 1) , \dots , M \parallel \alpha(r(i), v(i))\}$

$(1 \leq i \leq m)$ となるようなものを選び、さらに、予め定めた閾値の個数 k 個の部分デジタル署名作成部 13 の識別番号からなる 1 以上である s 個の集合

$I_1 , \dots , I_s \subseteq \{r(1) , \dots , r(m)\}$

を選び、それらに対して 1 以上である s 個の統合デジタル署名

$S(M', I_1) , \dots , S(M', I_s)$

を作成する。

【0060】

付加情報結合部 12 が結合する付加情報としては、デジタル署名作成機関の識別情報、デジタル署名の有効期限、デジタル署名作成の時刻、及びそれらの組み合わせ等が考えられる。

【0061】

【実施例】

以下、図面と共に本発明の実施例を説明する。

【0062】

以下、前述の図 3、図 4、図 5 を用いて、デジタル署名作成について、1 例をあげて説明する。なお、ここでは、公開鍵暗号の具体例として、RSA を用いる。RSA については、R.L. Rivest, A. Shamir, and L. Adleman 「A method for obtaining digital signature and public key cryptosystems」Communications of ACM, Vol.21, pp.294-299, 1978 に詳述されている。

最初に、部分署名作成のための部分デジタル署名作成部間の準備手順について説明する。

まず、 N を十分大きな 2 つの素数の積とし、 $\phi(N)$ を $0 \leq i < N$ で N と互いに素な整数 i の個数とする。次に、 e を部分デジタル署名作成部 13 の個数 r より小さい因数をもたなくかつ $\phi(N)$ と互いに素な整数とする。

【0063】

N と e の組 (N, e) を公開鍵とする。

【0064】

$$e \cdot (d_1 + \dots + d_r) \equiv 1 \pmod{\phi(N)}$$

となる整数の組 d_1, \dots, d_r を、D.Boneh et al.: Efficient generation of shared RSA key(extended abstract), in "Proceedings Crypto'97(Sprinter,97)で提案されている方法等を用いて分散生成し、各 $i = 1, \dots, r$ に対して部分デジタル署名作成部13が d_i を保持するようにする。

【0065】

ここで、

$$d = (d_1 + \dots + d_r)$$

と置くと、これが公開鍵 (N, e) に対応する秘密鍵になる。但し、各々の部分デジタル署名作成部13 i 、図3、図4、図5の部分デジタル署名作成部13 i は d_i を知るのみであり、どの部分デジタル署名作成部13も知ることはなく、かつ統合デジタル署名作成部14も d を知ることはない。

【0066】

k を分散署名作成のために必要となる部分署名の最低限の数、即ち、閾値とし、各部分デジタル署名作成部13 i は k 個の十分大きな整数係数

$$a_{i,0} = d_i, a_{i,1}, \dots, a_{i,k-1}$$

を選び、多項式 $f_i(x)$ を

$$f_i(x) = a_{i,0} + a_{i,1} \cdot x + \dots + a_{i,k-1} \cdot x^{k-1}$$

と置く ($1 \leq i \leq r$)。

【0067】

各部分デジタル署名作成部13 i は、 $1 \leq j \leq r$ かつ、 $j \neq i$ なる整数 j に対して、

$$f_i(j)$$

を計算し、部分デジタル署名作成部13 j に送信し、また、 $f_i(i)$ を計算する。

【0068】

各部分デジタル署名作成部13 i は、他の各部分デジタル署名作成部13 j から送られてきた $f_i(i)$ の値 ($j \neq i$ かつ $1 \leq j \leq r$) と、自分で計算し

た $f_i(i)$ の和を計算し、 $D(i)$ と置く。即ち、

【0069】

【数1】

$$D(i) = \sum_{j=1}^r f_j(i)$$

と置く。

【0070】

$D(i)$ を、部分デジタル署名作成部 13i の部分署名鍵と呼ぶ ($1 \leq i \leq r$)。

【0071】

次に、各部分デジタル署名作成部 13 における部分デジタル署名作成の手順について説明する。

【0072】

図3及び図4の構成では、各部分デジタル署名作成部 13i は、値域が $\{0, 1, \dots, N-1\}$ に含まれるような適当なハッシュ関数 H (例えば、SHA-1, やMD5) を用いて入力されたデジタル文書 M に対して

$$S_i(M) = H(M)^{D(i)} \bmod N$$

を計算し、これを M に対する部分デジタル署名とする ($1 \leq i \leq r$)。

【0073】

図5の構成における各部分デジタル署名作成部 13i は、値域が $\{0, 1, \dots, N-1\}$ に含まれるような適当なハッシュ関数 (例えば、SHA-1 やMD5) H を用いて付加情報結合部 12 から出力された付加情報付デジタル文書 $M \parallel \alpha(i, j)$ に対して、

$$S_i(M \parallel \alpha(i, j)) = H(M \parallel \alpha(i, j))^{D(i)} \bmod N$$

を計算し、これを $M \parallel \alpha(i, j)$ に対する部分デジタル署名とする ($i \leq i \leq r$)。

【0074】

次に、統合デジタル署名作成部 14 における統合デジタル署名作成の手順

について説明する。

【0075】

図3、図4の部分デジタル署名作成部13iが作成する部分デジタル署名 $S_i(M)$ に対して、Mを当該部分デジタル署名の被署名デジタル文書と呼ぶ。図5の部分デジタル署名作成部13iが作成する部分デジタル署名

$$S_i(M \parallel \alpha(i, j))$$

に対しては、付加情報付デジタル文書 $M \parallel \alpha(i, j)$ を当該部分デジタル署名の被署名デジタル文書と呼ぶ。

【0076】

$1 \leq r(1), \dots, r(k) \leq k \leq r$ で $r(1), \dots, r(k)$ は互いに異なり

$$S_{r(1)}(M'), \dots, S_{r(k)}(M')$$

を閾値個数の部分デジタル署名の集合で、各々被署名デジタル文書が M' に一致するものとするとき、統合デジタル署名作成部14が部分デジタル署名

$$S_{r(1)}(M'), \dots, S_{r(k)}(M')$$

を基に、統合デジタル署名 $S(M', I)$ を作成する手順は以下の通りである。

$I = \{r(1), \dots, r(k)\}$ とおき、さらに、各 $i \in I$ に対して

【0077】

【数2】

$$\lambda(I, i) = \prod_{j \in I, j \neq i} \frac{j}{j - i}$$

と置く。

【0078】

正整数 $\Delta(I)$ を e と互いに素で、かつ各 $i \in I$ について、

$$\Delta(I) \cdot \lambda(I, i)$$

が整数となるように選ぶ。以下、 $\Delta(I)$ を I についての部分デジタル署名の変換指数と呼ぶ。このような変換指数としては、例えば、『S.Miyazaki, K.Sakurai, M.Yung 「On threshold RSA-signing with no dealer」 in Proceedings of

f ICISC799, pp.197-207, Sprinter, 1999』に提案されているように、Iによらず、常に $((r-1)!)^2$ を選ぶことができるが、以下に述べるように総合デジタル署名作成の処理量が小さくなるような他の取り方も可能である。

【0079】

各 $i \in I$ に対して、

$$\Lambda(I, i) = \Delta(I) \cdot \lambda(I, i)$$

を計算する。

【0080】

部分デジタル署名に対して $Sr(i)(M')$ の $\Lambda(I, i)$ 乗を mod N でとるという変換処理を施し、その結果を $Tr(i)(M')$ とおく。即ち、

【0081】

【数3】

$$Tr(i)(M') = Sr(i)(M')^{\Lambda(I, i) \bmod N}$$

と置く。

【0082】

$Tr(1)(M'), \dots, Tr(k)(M')$ を乗算し、

【0083】

【数4】

$$w(I) = \left(\prod_{i \in I} Tr(i)(M') \right) \bmod N$$

を計算する。

【0084】

$\Delta(I)$ は、e と互いに素であるので、拡張ユークリッド互除法を用いて、

$$\Delta(I) \cdot a(I) + e \cdot b(I) = 1$$

となるような整数 $a(I)$ と $b(I)$ が計算可能である。これらを計算する。

【0085】

上記の $a(I)$, $b(I)$, $w(I)$ を用いて、

$$S(M', I) = w(I) \cdot a(I) \cdot H(M')^{b(I)} \bmod N$$

を計算し、これを被署名デジタル文書 M' に対する統合デジタル署名とする。

【0086】

図6は、本発明の一実施例の処理量が最小となるような部分デジタル署名に対する変換指数の計算手順を示す図である。

【0087】

上記の部分デジタル署名から統合デジタル署名を作成する処理において、
各々の閾値個数の部分デジタル署名作成部13の識別番号の集合

$$I = \{r(1), \dots, r(k)\}$$

に対して変換指数と呼ばれる正整数 $\Delta(I)$ を e と互いに素で、かつ各 $i \in I$ について、

$$\Delta(I) \cdot \lambda(I, i)$$

が整数となるように選ぶことが必要である。このような変換指数の取り方としては、『S. Miyazaki et al. 「On threshold RSA-signing with no dealer」 in Proceedings of ICISC'99, LNCS Vol.1787, pp. 197-207, Springer, 1999』において、 I によらず、常に $r-1$ の階乗の2乗、即ち、 $((r-1)!)^2$ をとることが提案されている。ここで、 r は、部分署名作成機関の総数である。図6は、部分デジタル署名作成部13の識別番号の集合 I に応じて、部分デジタル署名から統合デジタル署名を作成するために必要な処理量が最小となるという意味で最適となるような変換指数をとる手順を示したものである。閾値個数の部分デジタル署名作成部13の識別番号の集合 $i = \{r(1), \dots, r(k)\}$ が与えられたものとする。

【0088】

第1のステップ41において、各 $i \in I$ に対して、

【0089】

【数5】

$$\lambda(I, i) = \prod_{j \in I, j \neq i} \frac{j}{j-i}$$

を計算する。

【0090】

第2に、ステップ42において、各 $i \in I$ に対して、 $\lambda(I, i)$ を約分し、その結果の分母の絶対値を $\delta(I, i)$ とおく。即ち、

【0091】

【数6】

$$\lambda(I, i) = \frac{\gamma(I, i)}{\delta(I, i)}$$

で、 $\delta(I, i) > 0$ 、 $\gamma(I, i)$ と $\delta(I, i)$ は互いに素な整数となるように $\delta(I, i)$ を決める。

【0092】

第3に、ステップ43において、 $\delta(I, r(1)), \dots, \delta(I, r(K))$ の最小公倍数を計算し、 $\Delta(I)$ とおく。

【0093】

以上により、 I についての部分デジタル署名の変換指数 $\Delta(I)$ が得られる。 $\Delta(I)$ は、これを用いて部分デジタル署名から統合デジタル署名を作成するために必要な処理量が最小になるという意味で最適なものとなっている。例えば、『S.Miyazaki et al. 「On threshold RSA-signing with no dealer」 in Proceedings of ICISC'99, LNCS Vol.1787, pp. 197-207, Springer, 1999』で提案されているように部分デジタル署名部の総数を r として

$$\Delta(I) = ((r-1)!)^2$$

とする場合に比較すると、署名に必要な閾値 k が3から10で部分署名作成部13の数 r が5から19の場合、部分デジタル署名から統合デジタル署名を作成する処理量が約1/6倍に減少することが計算により確認できる。

【0094】

次に、不正な部分デジタル署名の存在の判定手順について説明する。

【0095】

図7は、本発明の一実施例の部分デジタル署名の組み合わせによる不正な部分デジタル署名の検出法を説明するための図である。また、図8は、本発明の一実施例の部分デジタル署名の組み合わせによる不正な部分デジタル署名存在の判定手順のフローチャートであり、図9は、本発明の不正な部分デジタル署名が1個のみか否かを判定し、1個のみ存在する不正な部分デジタル署名を決定する手順のフローチャートである。

【0096】

これらを用いて、図3、図4、図5で示された閾値分散デジタル署名作成装置において、統合デジタル署名作成部14が部分署名を閾値の個数だけ組み合わせ署名検証処理を施すことにより、不正な部分署名鍵を用いて作成された不正な部分署名の存在を判定し、かつ不正な部分署名を特定する手順について説明する。

【0097】

k を部分デジタル署名から統合デジタル署名を作成するために必要な閾値としたとき、図3、図4、図5の統合デジタル署名作成部14は、各々異なる部分署名作成部13から出力されたもので、かつ被署名デジタル文書が一致するような k 個の部分デジタル署名、

$$Sr(1)(M'), \dots, Sr(k)(M')$$

$(r(1), \dots, r(k))$ は互いに異なり、 $1 \leq r(1), \dots, r(k) \leq r$ から統合デジタル署名

$$S(M', I)$$

を作成することができる。ここで、 M' は、 $Sr(k)(M')$ の被署名デジタル文書とし、 $I = \{r(1), \dots, r(k)\}$ とおく。

【0098】

このような k 個の部分デジタル署名の種々の組み合わせに対して、統合デジタル署名作成部14は、作成された $S(M', I)$ が被署名デジタル文書 M

の署名になっているか否かを、公開鍵 (e, N) による $S(M', I)$ の復号化が被署名デジタル文書のハッシュ値 $H(M')$ に一致するか否かを試験することにより判定する。このことにより、 $S(M', I)$ が最初に与えられたデジタル文書の正しいデジタル署名となっているか否かを判定することができる。

【0099】

先に述べたように、デジタル署名 $S(M', I)$ の被署名デジタル文書 M' は、付加情報が無い図3及び図4の構成のときは、 M であり、付加情報 α がある図5の構成のときは、 $M \parallel \alpha$ である。

【0100】

被署名デジタル文書 M' は、図3の構成においては、最初から統合デジタル署名作成部13に入力されるものであり、図4、図5の構成においては、部分デジタル署名 $S_i(M')$ と対になって部分デジタル署名作成部13、図4及び図5の部分デジタル署名作成部13 i ($1 \leq i \leq r$) から統合デジタル署名作成部14に出力されるものである。

【0101】

図8を用いて、図3、図4、図5の各々の部分デジタル署名作成部13 i から送信されてきた、被署名デジタル文書が M' に一致する、部分デジタル署名の集合

$$S_{r(1)}(M'), \dots, S_{r(m)}(M')$$

の中に、正しい部分署名が少なくとも総合署名作成のために必要な閾値 k より1小さい数だけある場合に、

$$S_{r(1)}(M'), \dots, S_{r(m)}(M')$$

の中に不正な部分署名が存在するか否かを判定する手順を示す。

【0102】

但し、 $k+1 \leq m \leq r$ で、 $r(1), \dots, r(m)$ は互いに異なるものとする。ここで、 $m=r$ としないのは、部分デジタル署名作成部13の一部が正常に動作せず、部分デジタル署名を送信しない可能性があるからである。

【0103】

ステップ61) 図7に示すように、 m 個の個数 k の $\{r(1), \dots, r(m)\}$ 部分集合 $I(0), \dots, I(m-1)$ を選ぶ。

【0104】

$I(i) = \{r((j+1) \bmod m) + 1 \mid 0 \leq j \leq m-1\}$
(但し、 $i = 0, \dots, m-1$)

ステップ62) 各 $I(i)$ ($i = 0, \dots, m-1$) に対して

$$\{Sr(M') \mid r \in I(i)\}$$

から統合デジタル署名 $S(M', I(i))$ を作成する。

【0105】

ステップ63) 各 $I(i)$ ($i = 0, \dots, m-1$) に対して、当該統合デジタル署名の公開鍵 (e, N) による復号化

$$S(M', I(i))^e \bmod N$$

が $H(M')$ に一致するかどうかを試験する。

【0106】

ステップ64) 全ての $I(i)$ ($i = 0, \dots, m-1$) に対して、上記ステップ63で

$$S(M', I(i))^e \bmod N = H(M')$$

が成り立つことを確認できれば、

$$Sr(i)(M'), \dots, Sr(m)(M')$$

の中に不正な部分署名が存在すると判定する。

【0107】

m 個の部分デジタル署名

$$Sr(1)(M'), \dots, Sr(m)(M')$$

のなかに不正な部分デジタル署名が複数あり、それらが結託して互いの不正の効果を打ち消しあうことにより、 $0 \leq i \leq m-1$ なる各 $I(i)$ について、 $Sr(M')$ ($r \in I(i)$) から生成される統合デジタル署名 $S(M', I(i))$ が正当な署名となるという可能性も想定されるが、 $3 \leq k \leq 10$ で $k+1 \leq r \leq 2 \cdot k - 1$ という範囲ではこのようなことは起こらないことが計算機テストにより確認できる。

【0108】

次に、不正な部分デジタルが1個のみか否かの判定と1個のみ存在する不正な部分デジタル署名の決定手順について説明する。

【0109】

図9において、 m 個の部分デジタル署名

$$Sr(1)(M'), \dots, Sr(m)(M')$$

の中に、正しい部分署名が少なくとも総合デジタル署名作成のために必要な閾値 k 個だけあり、かつ、図8に示す手順により、

$$Sr(1)(M'), \dots, Sr(m)(M')$$

の中に不正なデジタル署名があると判定された場合に、その中の不正な部分デジタル署名が1個のみか否かを判定し、1個のみ存在すると判定された場合に、その不正な部分デジタル署名を決定する手順を示す。

【0110】

$$\text{ステップ71)} \quad S(M', I(i))^e \bmod N = H(M')$$

が成り立たないような i ($0 \leq i \leq m-1$) の集合を F とおく。この判定は、上記の図8のステップ63でも行ったものであり、図8の手順を実行するときに、同時にこのステップを実行してもよい。

【0111】

ステップ72) $0 \leq i \leq m-1$ なる各 i に対して、

$$F(i) = \{j \mid 0 \leq j \leq m-1 \text{ かつ } r(i) \in I(j)\}$$

とおく。

【0112】

ステップ73) $0 \leq i \leq m-1$ なるある j が存在して、 $F = F(i)$ が成り立つならば、不正な部分署名は $Sr(i)(M')$ のみであると決定する。さもなければ、

$$Sr(1)(M), \dots, Sr(m)(M)$$

の中には、不正な部分署名が2個以上あると判定する。

【0113】

$F = F(j)$ となるような ($0 \leq j \leq m-1$) はあるとしても高々1つである

。m個の部分デジタル署名

$$Sr(1)(M'), \dots, Sr(m)(M')$$

の中に不正な部分デジタル署名が複数あり、それらが結託して互いの不正の効果を打ち消しあうことにより、上記のステップ74において、 $1 \leq i \leq m$ なるある i について、 $F = F(i)$ となる可能性も想定できるが、 $3 \leq k \leq 10$ で $k+1 \leq r \leq 2 \cdot k - 1$ という範囲ではこのようなことは起こらないことが計算機テストにより確認できる。

【0114】

上記の処理における処理量を評価する。

【0115】

k を統合デジタル署名を作成するために必要な部分デジタル署名デジタル署名の数、即ち、閾値とし、 r を部分デジタル署名作成部の数とし、 $3 \leq k \leq 10$ とし、各 k に対して $r = 2 \cdot k - 1$ としたとき、鍵の長さが2048ビットの場合には、上記の手順で不正な部分デジタル署名の存在の判定、及び不正な部分デジタル署名が存在すると判定されたときに、不正な部分デジタル署名が1つのみか否か、及び不正な部分デジタル署名が1つのみと判定されたときに不正な部分デジタル署名を決定するための処理量を $\text{mod } N$ での乗算の数で評価すると、 $k = 3$ のときは、部分署名に必要な処理量の0.10倍、 $k = 4$ のときは、部分署名に必要な処理量の0.17倍、 $k = 5$ のときは、部分署名に必要な処理量の0.28倍、 $k = 6$ のときは、部分署名に必要な処理量の0.44倍、 $k = 7$ のときは部分署名に必要な処理量の0.69倍、 $k = 8$ のときは部分署名に必要な処理量の0.98倍、 $k = 9$ のときは、部分署名に必要な処理量の1.4倍、 $k = 10$ の時は、部分署名に必要な処理量の2.0倍となる。

【0116】

従来、『T.Wu et al. 「Building intrusion tolerant applications」, in Proceedings of 8th USENIX Security Symposium, USENIX, 1999』で提案されている検証法や、『S.Miyazaki et al. 「On threshold RSA-signing with no dealer」 in Proceedings of ICISC'99, LNCS Vol. 1787, pp. 197-207, Springer, 1999』で提案されている検証法では、部分デジタル署名作成部が部分ディジタ

ル署名以外に、部分署名の正当性を検証するためのデータを追加して生成して、統合デジタル署名部に送信し、それを受信した統合デジタル署名部が個々の部分デジタル署名の正当性を検証するために、部分署名作成の2倍以上の処理量を要している。従って、統合デジタル署名作成に必要な k 個の部分デジタル署名の正当性検証に必要な処理量は、 $k=3$ のときは、部分署名に必要な処理量の6倍以上、 $k=4$ の時は、部分署名に必要な処理量の8倍以上、 $k=5$ のときは、部分署名に必要な処理量の10倍以上、 $k=6$ のときは、部分署名に必要な処理量の12倍以上、 $k=7$ のときは、部分署名に必要な処理量の14倍以上、 $k=8$ のときは、部分署名に必要な処理量の16倍以上、 $k=9$ のときは、部分署名に必要な処理量の18倍以上、 $k=10$ のときは、部分処理に必要な処理量の20倍以上となる。

【0117】

上記の2つの処理量の評価を比較すると、本発明における不正な部分署名の検証方法は、上記の鍵長、閾値の数、及び部分デジタル署名部の総数に対しては、必要な処理量が少ないという利点を持っていることがわかる。

【0118】

次に、全ての可能な統合デジタル署名の作成法を用いる場合について説明する。

【0119】

また、部分デジタル署名作成部の数が小さいときには、各々異なる部分デジタル署名作成部により作成され、被署名デジタル文書が一致するような部分署名の集合

$$Sr(1)(M'), \dots, Sr(m)(M')$$

に対して、 $\{r(1), \dots, r(m)\}$ の個数 k 個の全ての部分集合

$$J(1), \dots, J(K)$$

に対して、

【0120】

【数 7】

$$S(M', J(i)) \pmod{N} = H(M)$$

が成り立つか否かを試験し、 $J(i)$ と当該試験結果との対応付けを検査することにより、不正な部分署名が2個以上あってもそれらを特定できる場合がある。

ここでKは、m個からk個を選ぶ組み合わせの総数

$$m! / (k! \cdot (m-k)!)$$

である。例えば、統合デジタル署名作成のための閾値が3で、部分デジタル署名作成部の総数が5、かつ被署名デジタル文書が一致する部分デジタル署名が5個集まったときには、不正な部分署名が高々2個あっても、どの部分署名が不正かを決定することができることが、全ての場合を数え上げることにより確認できる。

【0 1 2 1】

次に、図10、図11を用いて閾値個数の部分署名の組み合わせによる分散デジタル署名付デジタル文書作成装置について説明する。

【0 1 2 2】

図10は、本発明の一実施例の閾値個数の部分署名の組み合わせによる分散デジタル署名付デジタル文書作成装置の構成図（その1）であり、図11は、本発明の一実施例の閾値個数の部分署名の組み合わせによる分散デジタル署名付デジタル文書作成装置の構成図（その2）である。

【0 1 2 3】

図10及び図11において、分散デジタル署名付デジタル文書作成装置2は、複数の部分デジタル署名作成部131, ..., 13r、統合デジタル署名作成部14、及び、デジタル署名付デジタル文書作成部15とを有する。

【0 1 2 4】

部分デジタル署名作成部131, ..., 13rは、入力されたデジタル文書Mに対して、各々独立に部分デジタル署名

$$S1(M), \dots, Sr(M)$$

を作成する。

【0125】

統合デジタル署名作成部 14 は、上記の複数の部分デジタル署名作成部 13 で独立に作成された m 個の部分デジタル署名

$$S_r(1)(M), \dots, S_r(m)(M)$$

($k \leq m \leq r$ かつ $k \leq r(1), \dots, r(m) \leq r$) 及び、当該デジタル文書 M を受け取り、予め定めた閾値の個数 k 個の部分デジタル署名作成部の識別番号からなる 1 以上である s の集合

$$I_1, \dots, I_s$$

に対して、出力された部分デジタル署名から複数の統合デジタル署名

$$S(M, I_1), \dots, S(M, I_s)$$

を作成する。

【0126】

デジタル署名付デジタル文書作成部 15 は、作成された統合デジタル署名と入力されたデジタル文書を組み合わせ、当該デジタル文書に対するデジタル署名付デジタル文書を作成する。

【0127】

次に、上記の図 10、図 11 の構成に付加情報結合部を設けた例を説明する。

図 12 は、本発明の一実施例の閾値個数の部分署名の組み合わせによる分散デジタル署名付デジタル文書作成装置の構成図（その 3）である。

【0128】

図 12 において、分散デジタル署名付デジタル文書作成装置 2 は、複数の付加情報結合部 121, ..., 12r と、複数の部分デジタル署名作成部 13、統合デジタル署名作成部 14 及びデジタル署名付デジタル文書作成部 15 から構成される。

【0129】

付加情報結合部 12 は、入力されたデジタル文書に各々独立に付加情報を付加し、付加情報付デジタル文書 18 を部分デジタル署名作成部 13 に出力する。

【0130】

部分デジタル署名作成部131, ..., 13r は、入力された付加情報付デジタル文書18の部分デジタル署名の組

$$(M \parallel \alpha(i, 1), S_i(M \parallel \alpha(i, 1))), \dots, \\ (M \parallel \alpha(i, v(i)), S_i(M \parallel \alpha(i, v(i)))) \\ (1 \leq i \leq r)$$

を作成する。

【0131】

統合デジタル署名作成部14は、複数の部分デジタル署名作成部13で独立の作成された付加情報付デジタル文書M' とその部分デジタル署名のm個の組

$$(M', S_{r(1)}(M')), \dots, (M', S_{r(m)}(M'))$$

($k \leq m \leq r$ かつ $1 \leq r(1), \dots, r(m) \leq r$) を受け取り、予め定めた閾値の個数k個の部分デジタル署名作成部13の識別番号からなる1以上のsの集合

$$I_1, \dots, I_s$$

に対して、出力された部分デジタル署名から1以上であるs個の統合デジタル署名

$$S(M', I_1), \dots, S(M', I_s)$$

を作成する。

【0132】

デジタル署名付文書作成部15は、作成された付加情報付デジタル文書とそれに対する統合デジタル署名を組み合わせ、当該付加情報付デジタル文書に対するデジタル署名付デジタル文書Tを作成する。

【0133】

また、上記の実施例では、各構成図に基づいて説明したが、図3～図5に示す分散デジタル署名作成装置の部分デジタル作成部、統合デジタル署名作成部及び、付加情報結合部についてプログラムとして構築することが可能であり、これらのプログラムを分散デジタル署名作成装置として利用されるコンピュー

タのCPUにインストールすることも可能である。

【0134】

また、構築されたプログラムをコンピュータに接続されるハードディスクや、フロッピーディスク、CD-ROM等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【0135】

また、図11、図12に示した分散デジタル署名付デジタル文書作成装置の作成装置の部分デジタル作成部、統合デジタル署名作成部及び、付加情報結合部及びデジタル署名付デジタル文書作成部についてプログラムとして構築することが可能であり、これらのプログラムを分散デジタル署名作成装置として利用されるコンピュータのCPUにインストールすることも可能である。

【0136】

また、分散デジタル署名作成装置と同様に、構築されたプログラムをコンピュータに接続されるハードディスクや、フロッピーディスク、CD-ROM等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【0137】

なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【0138】

【発明の効果】

上述のように、本発明の閾値型分散デジタル署名作成装置によれば、信頼される第三者機関を含まないことによりデジタル署名のための秘密鍵を中心とする秘密鍵の漏洩をもたらす秘密漏洩の単一点を除くことにより、秘密鍵の安全性を中心とする署名システムの安全性を向上させ、同時に、複数ある部分デジタル署名作成機関のうちの、予め定められた一定数が正常動作すれば、デジタル署名の作成を可能とすることにより、デジタル署名システムの耐攻撃性及び耐故障性を向上させ、これにより安全で、耐攻撃性及び耐故障性に優れた分散デジタル署名作成システムが実現できる。

【図面の簡単な説明】

【図 1】

本発明の原理を説明するための図である。

【図 2】

本発明の原理構成図である。

【図 3】

本発明の閾値個数の部分署名の組み合わせによる分散デジタル署名作成装置の構成図（その 1）である。

【図 4】

本発明の閾値個数の部分署名の組み合わせによる分散デジタル署名作成装置の構成図（その 2）である。

【図 5】

本発明の閾値個数の部分署名の組み合わせによる分散デジタル署名作成装置の構成図（その 3）である。

【図 6】

本発明の第 1 の実施例の処理量が最小となるような部分デジタル署名に対する変換指数の計算手順のフローチャートである。

【図 7】

本発明の第 1 の実施例の部分デジタル署名の組み合わせによる不正な部分デジタル署名の検出法を説明するための図である。

【図 8】

本発明の第 1 の実施例の部分デジタル署名の組み合わせによる不正な部分デジタル署名存在の判定手順のフローチャートである。

【図 9】

本発明の第 1 の実施例の不正な部分デジタル署名が 1 個のみか否かを判定し、1 個のみ存在する不正な部分デジタル署名を決定する手順のフローチャートである。

【図 1 0】

本発明の第 2 の実施例の閾値個数の部分署名の組み合わせによる分散ディジタ

ル署名付デジタル文書作成装置の構成図（その１）である。

【図 1 1】

本発明の第 2 の実施例の閾値個数の部分署名の組み合わせによる分散デジタル署名付デジタル文書作成装置の構成図（その 2）である。

【図 1 2】

本発明の第 2 の実施例の閾値個数の部分署名の組み合わせによる分散デジタル署名付デジタル文書作成装置の構成図（その 3）である。

【符号の説明】

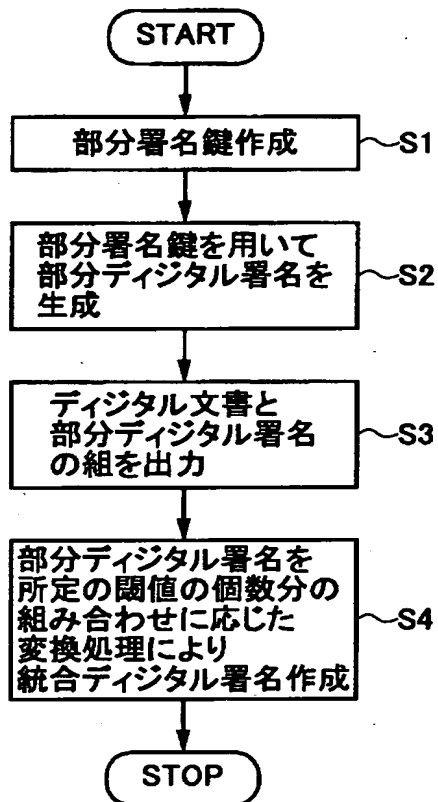
- 1 分散デジタル署名作成装置
- 2 分散デジタル署名付デジタル文書作成装置
- 1 2 付加情報結合部
- 1 3 部分デジタル署名作成手段、部分デジタル署名作成部
- 1 4 統合デジタル署名作成手段、統合デジタル署名作成部
- 1 5 デジタル署名付デジタル文書作成部
- 1 6 部分デジタル署名
- 1 7 デジタル文書と部分デジタル署名の組
- 1 8 付加情報付デジタル文書
- 1 9 付加情報付デジタル文書と部分デジタル署名の組
- M デジタル文書
- T デジタル署名付デジタル文書

【書類名】

図面

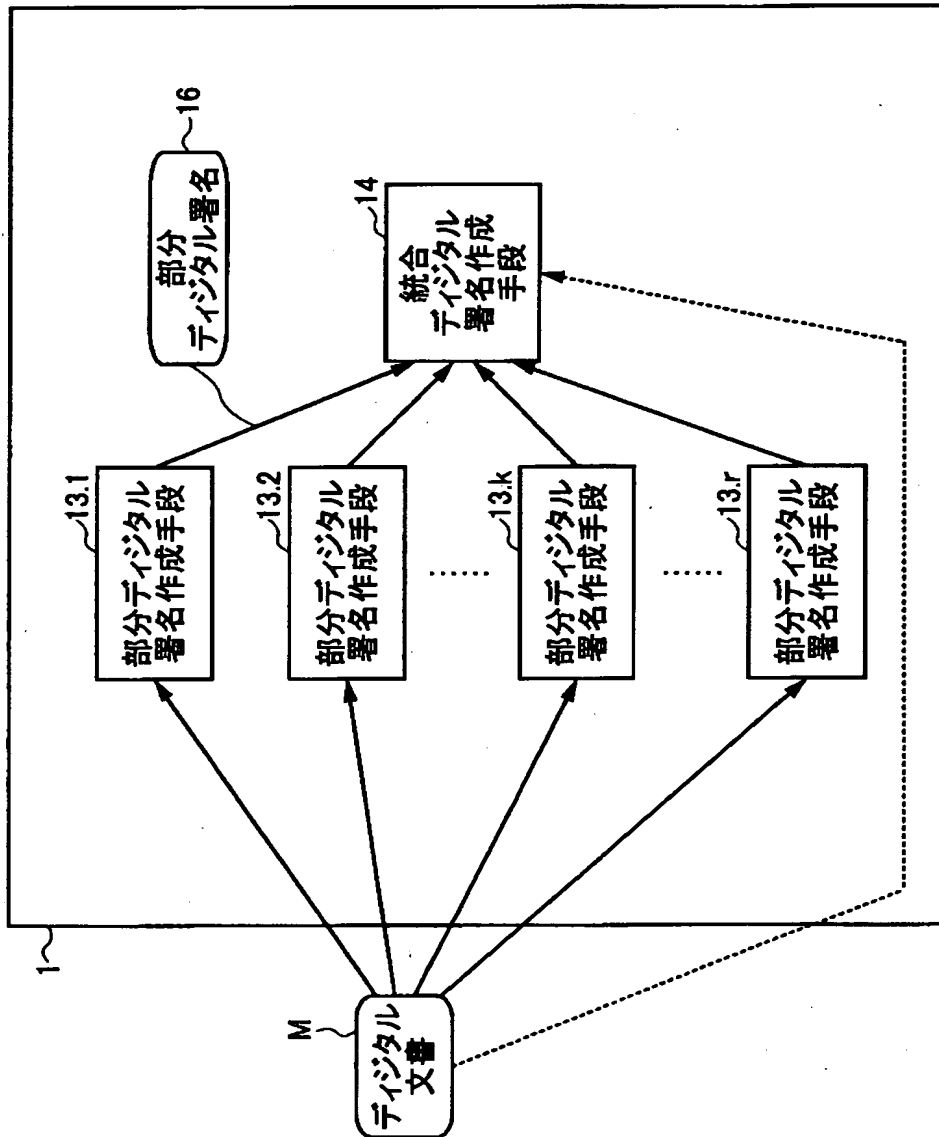
【図 1】

本発明の原理を説明するための図



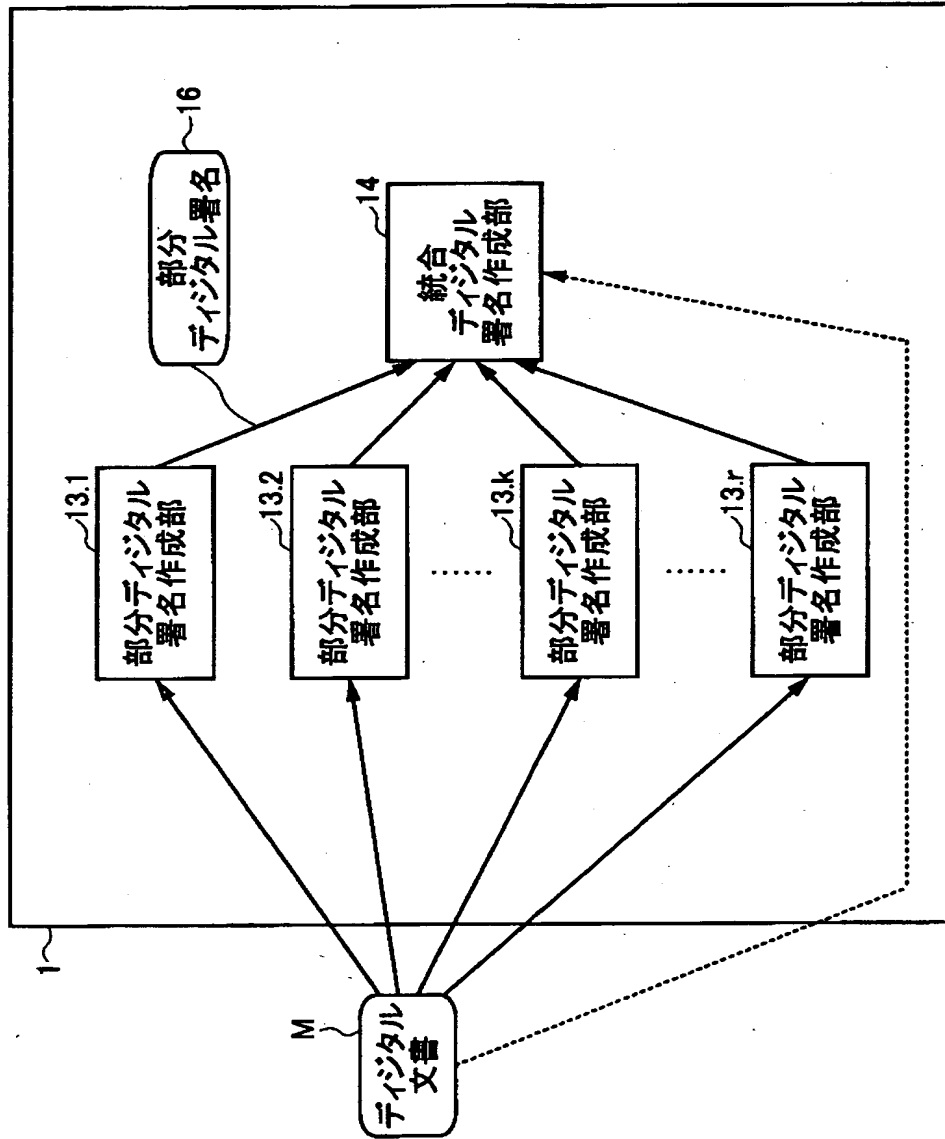
【図 2】

本発明の原理構成図



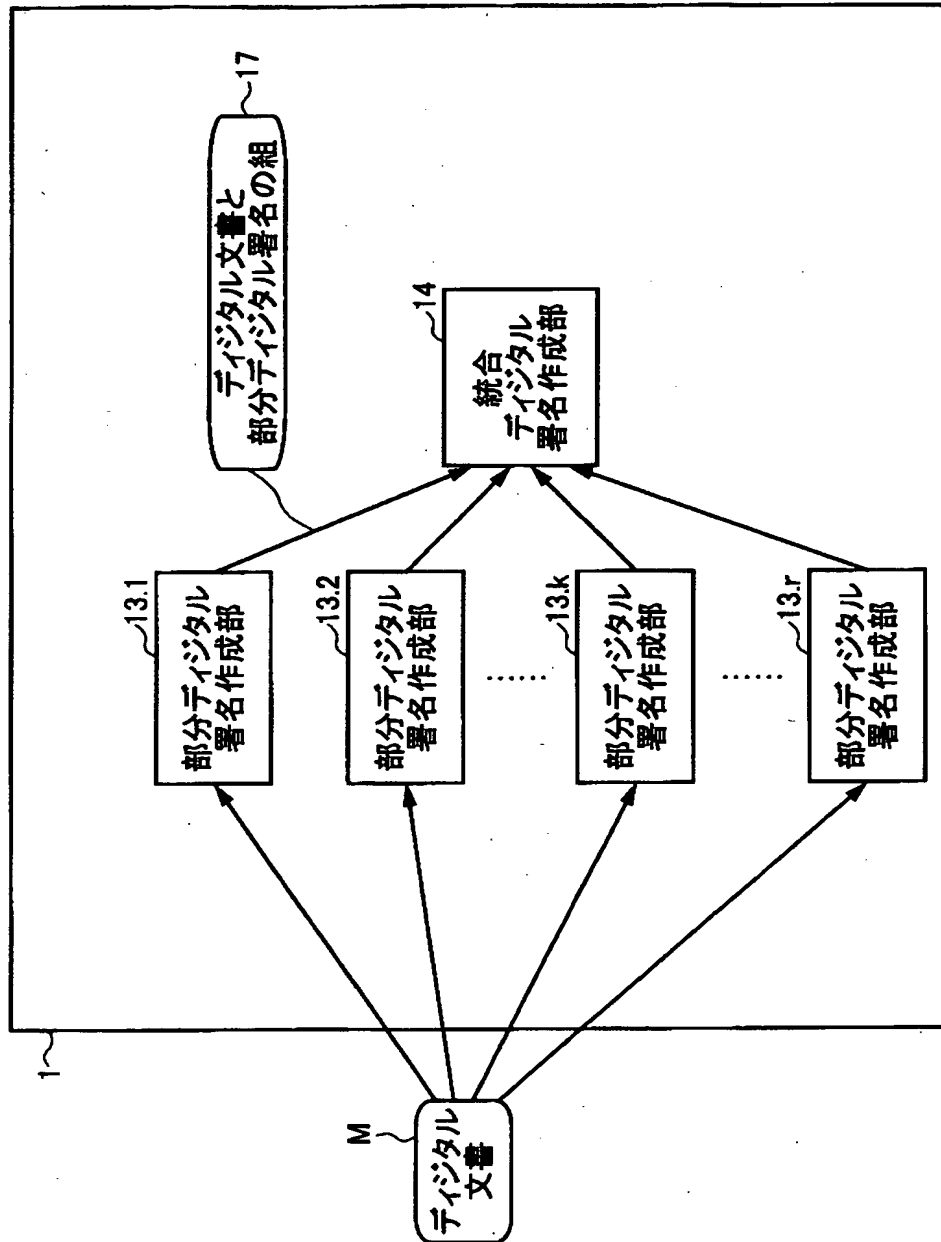
【図3】

本発明の閾値個数の部分署名の組合せによる
分散デジタル署名作成装置の構成図(その1)



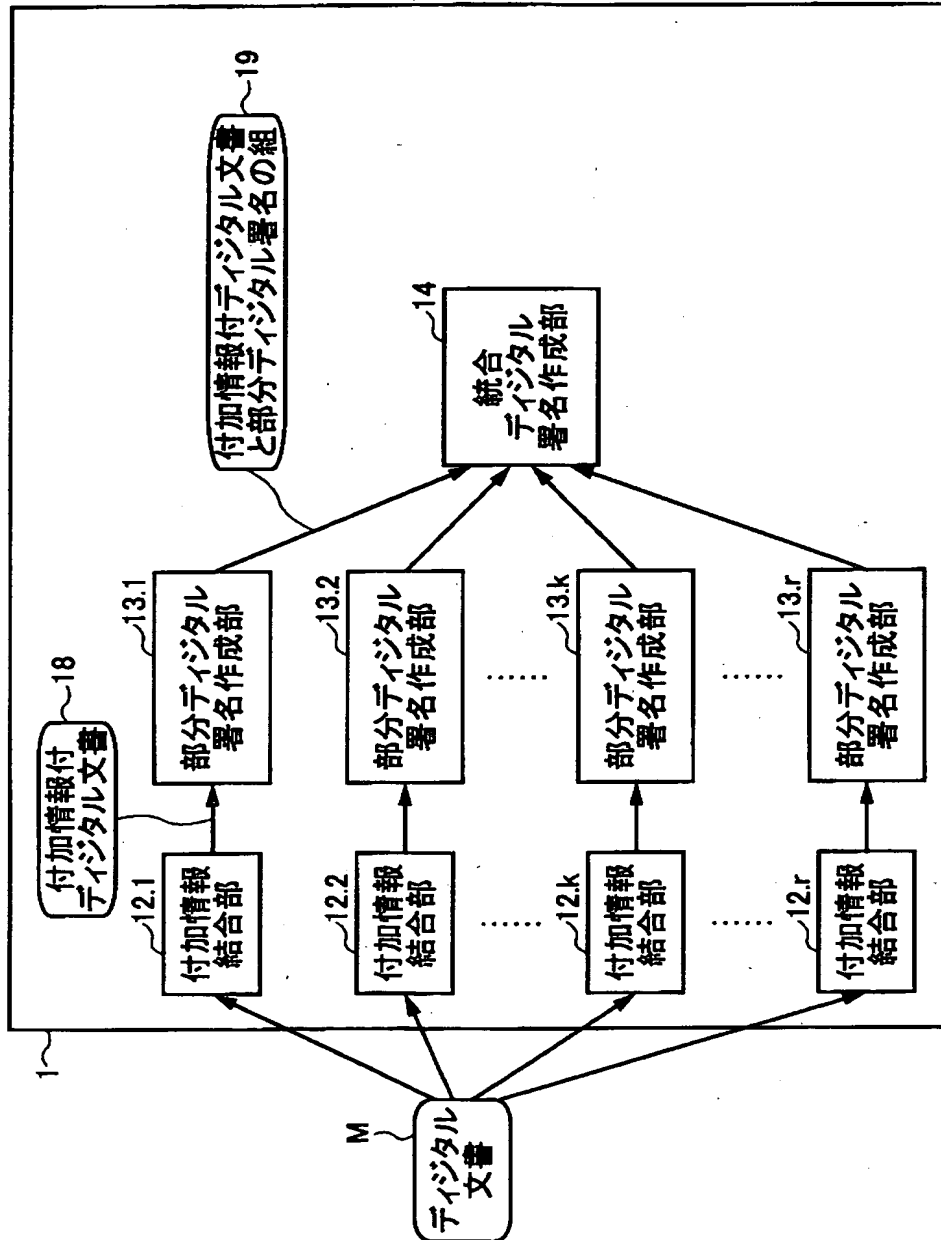
【図 4】

本発明の閾値個数の部分署名の組合せによる
分散デジタル署名作成装置の構成図(その2)



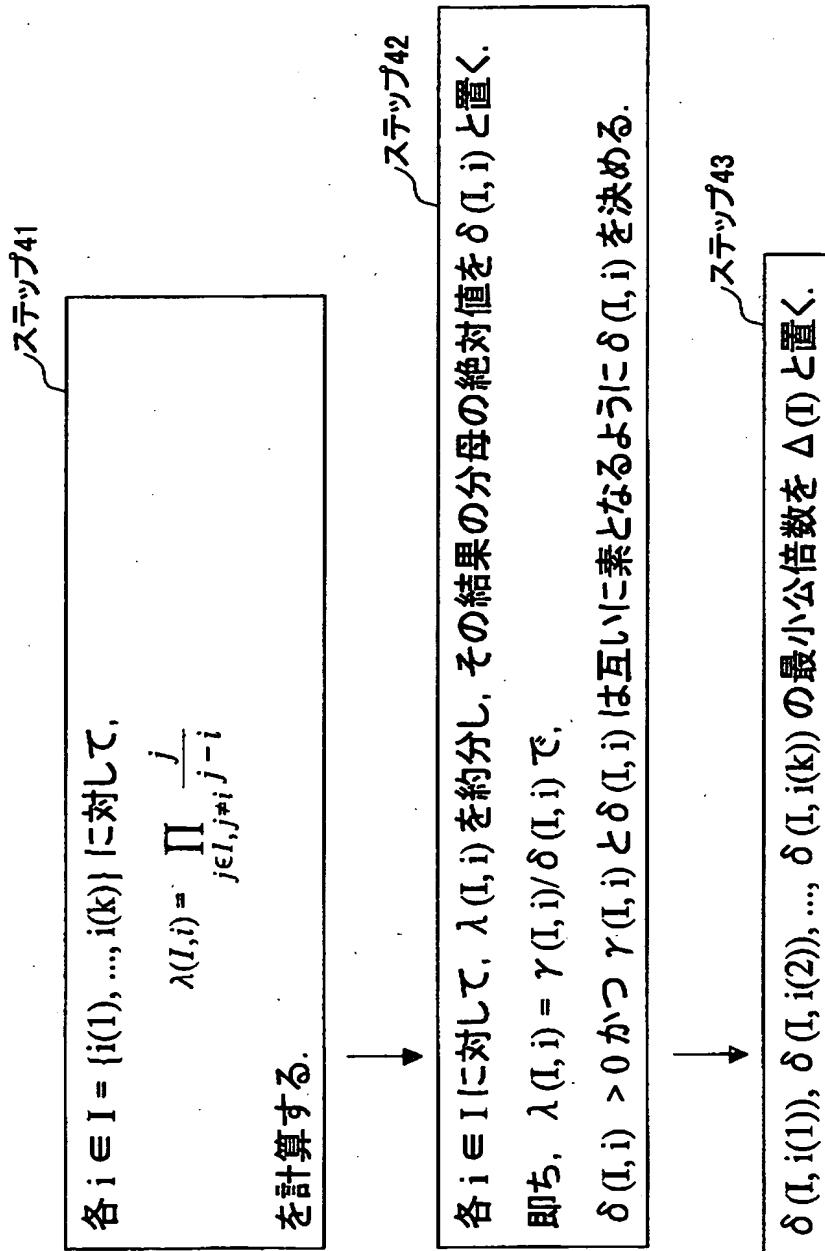
【図5】

本発明の閾値個数の部分署名の組合せによる
分散デジタル署名作成装置の構成図(その3)



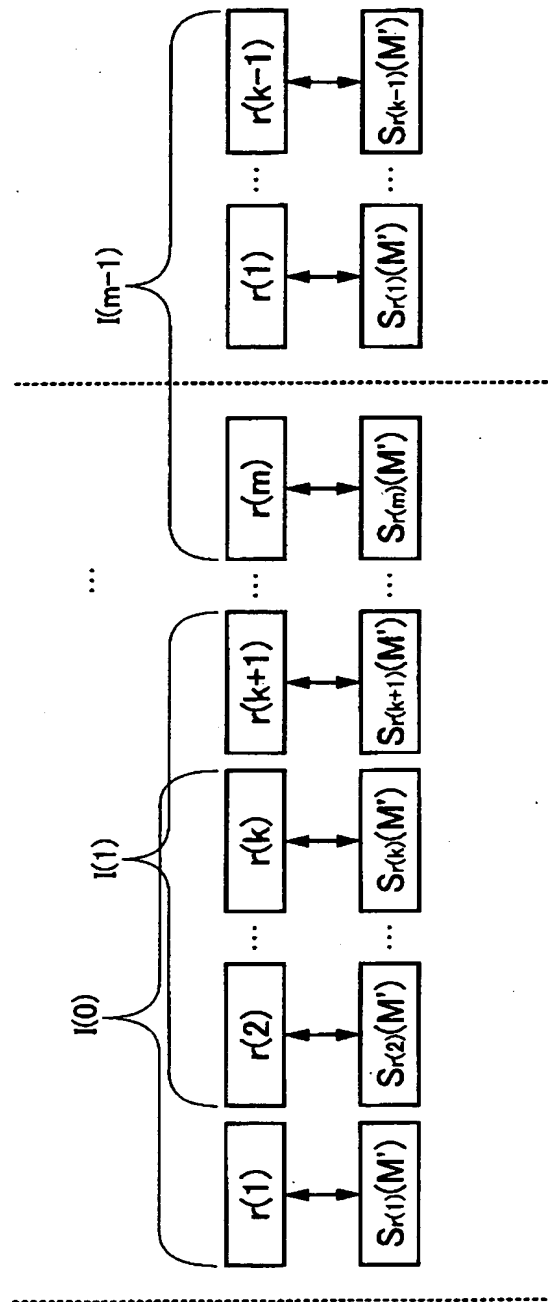
【図 6】

本発明の第1の実施例の処理量が最小となるような
部分デジタル署名に対する変換指数の計算手順のフローチャート



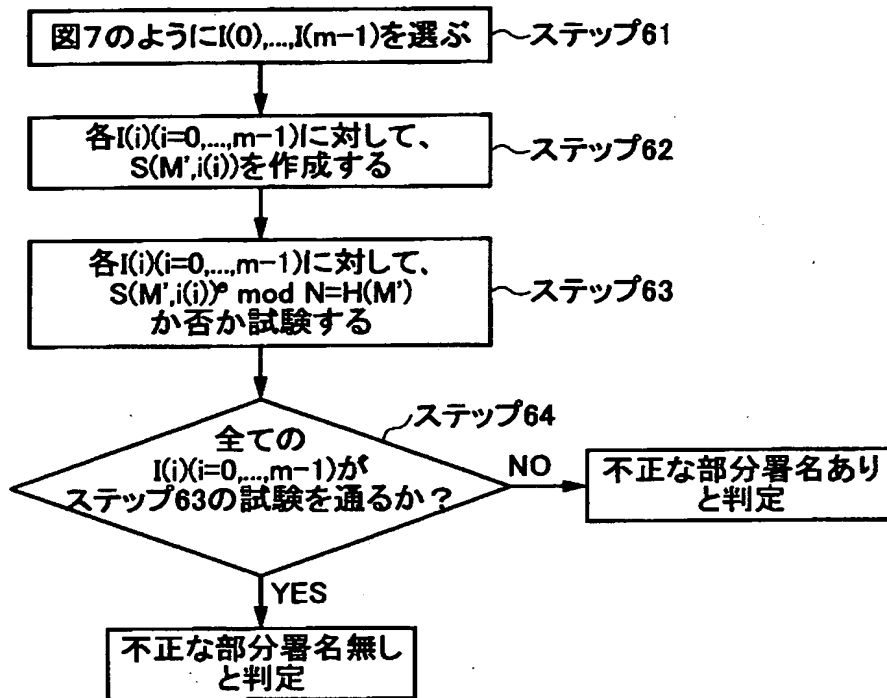
【図 7】

本発明の第1の実施例の部分デジタル署名の組合せによる不正な部分デジタル署名の検出法を説明するための図



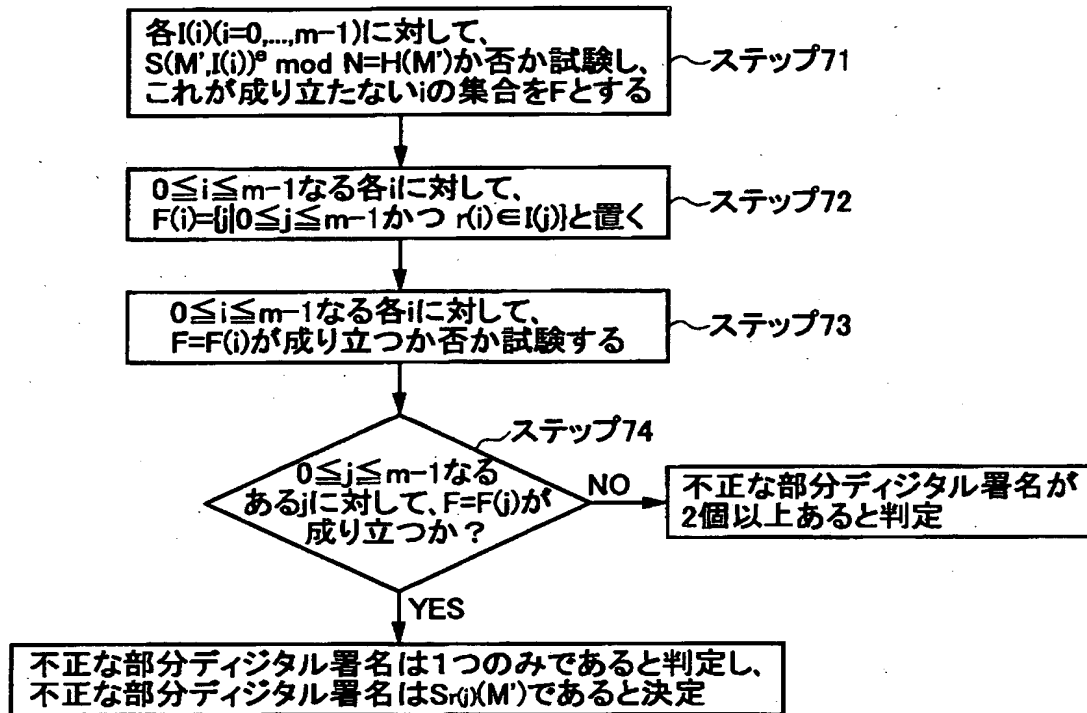
【図 8】

本発明の第1の実施例の部分デジタル署名の組合せによる不正な部分デジタル署名存在の判定手順のフローチャート



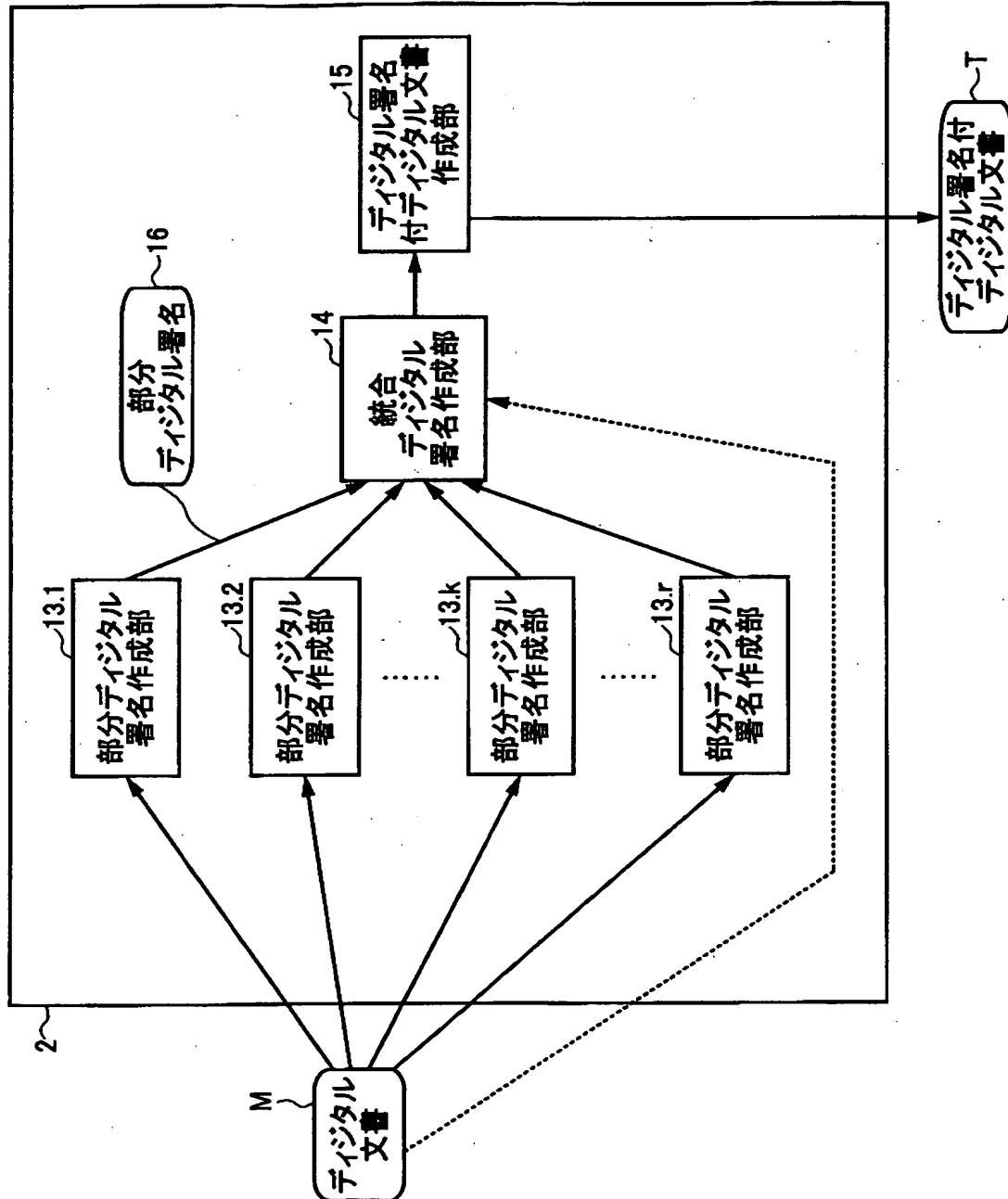
【図9】

本発明の第1実施例の不正な部分デジタル署名が1個のみか否かを判定し一個のみ存在する不正な部分デジタル署名を決定する手順のフローチャート



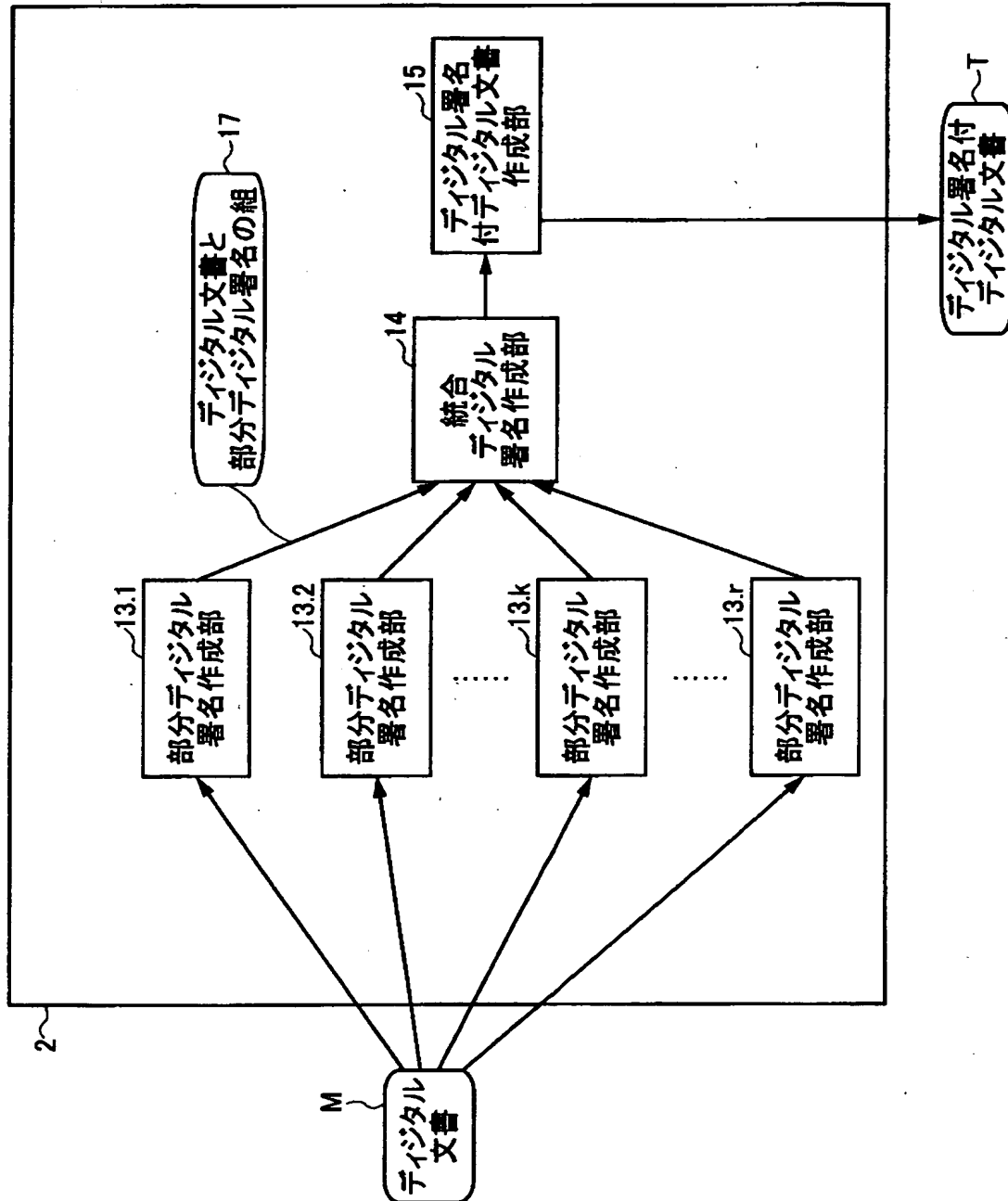
【図10】

本発明の第2の実施例の閾値個数の部分署名の組合せによる分散デジタル署名付デジタル文書作成装置の構成図(その1)



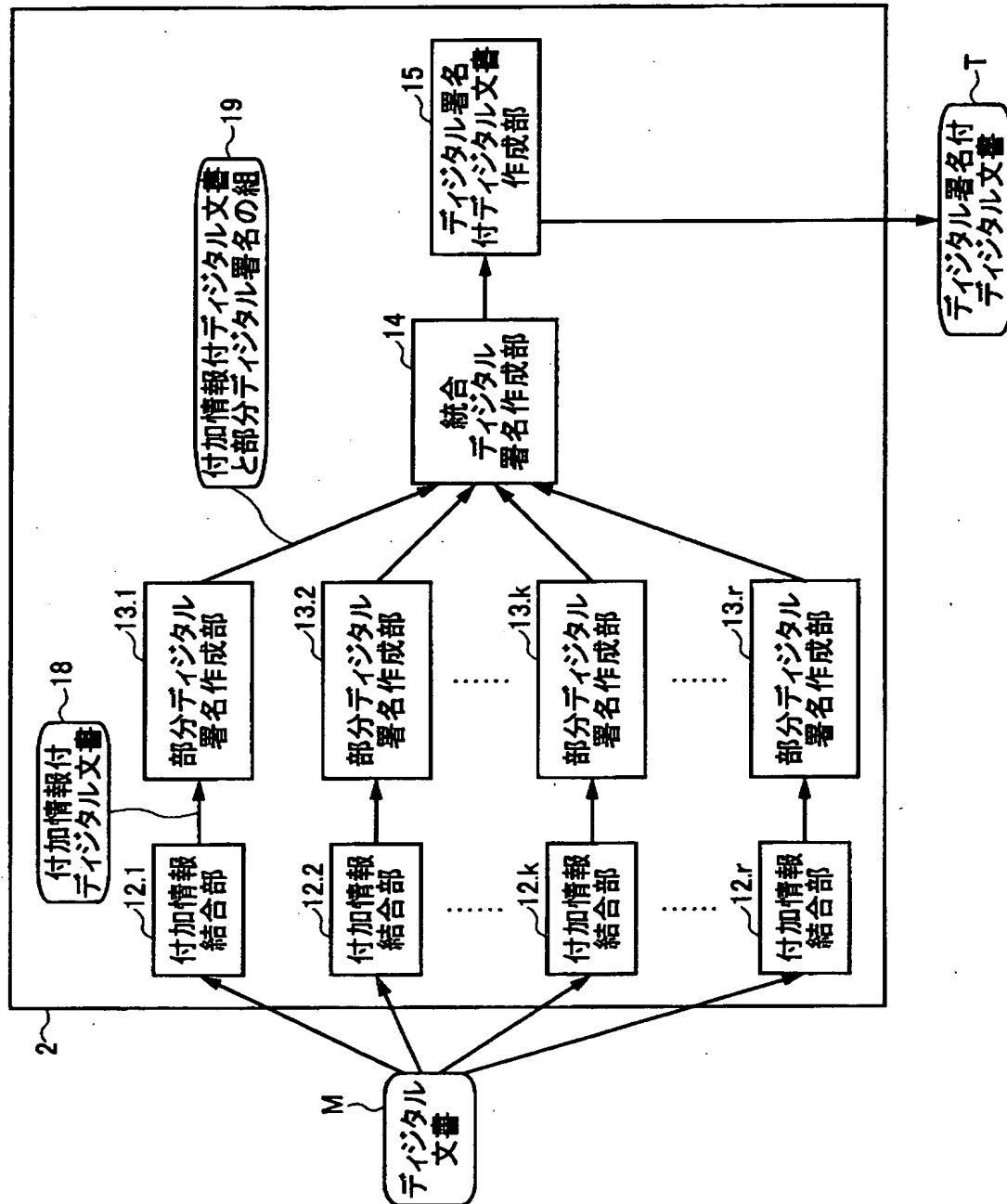
【図11】

本発明の第2の実施例の閾値個数の部分署名の組合せによる分散デジタル署名付デジタル文書作成装置の構成図(その2)



【図 1 2】

本発明の第2の実施例の閾値個数の部分署名の組合せによる分散デジタル署名付デジタル文書作成装置



【書類名】 要約書

【要約】

【課題】 秘密漏洩の単一点を存在させず、かつ、部分デジタル署名機関の全てのものが正しい部分デジタル署名を作成しなければデジタル署名が作成できないようにする。

【解決手段】 本発明は、入力されるデジタル文書のハッシュ値に対して分散処理により生成された部分署名鍵を用いて各々の部分デジタル署名を作成し、作成された部分デジタル署名あるいは入力されたデジタル文書とその部分デジタル署名の組を生成し、部分デジタル署名を予め定められた閾値の個数だけ組み合わせて変換処理を行ない、統合デジタル署名を作成する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号

[000004226]

1. 変更年月日 1999年 7月15日

[変更理由] 住所変更

住 所 東京都千代田区大手町二丁目3番1号

氏 名 日本電信電話株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.